Министерство образования Республики Беларусь

Учреждение образования
«Гомельский государственный технический
университет имени П. О. Сухого»

Кафедра «Нефтегазоразработка и гидропневмоавтоматика»

А. Б. Невзорова

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ НЕФТЕДОБЫВАЮЩЕЙ ОТРАСЛИ

УЧЕБНОЕ ПОСОБИЕ

Допущено Министерством образования
Республики Беларусь в качестве учебного пособия
для студентов учреждений высшего образования
по специальности магистратуры
«Нефтегазовый инжиниринг»

Электронный аналог печатного издания

Гомель 2025

УДК 622.276:004(075.8)
ББК 33.3я73
Н40

Рецензенты: кафедра «Программное обеспечение информационных технологий» Белорусско-Российского университета;
зав. каф. «Программное обеспечение информационных технологий» Белорусско-Российского университета канд. техн. наук, доц. *В. В. Кутузов*;
заместитель главного инженера по информационным технологиям РУП ПО «Белоруснефть» канд. физ.-мат. наук *Е. В. Коробейникова*

Невзорова, А. Б.

Н40 Цифровая трансформация производственных процессов нефтедобывающей отрасли : учеб. пособие / А. Б. Невзорова. – Гомель : ГГТУ им. П. О. Сухого, 2025. – 189 с. – Систем. требования: PC не ниже Intel Celeron 300 МГц ; 2 Gb RAM ; свободное место на HDD 16 Mb ; ALT Lunux 10.1 ; Adobe Acrobat Reader. – URL: https://elib.gstu.by. – Загл. с титул. экрана.

ISBN 978-985-535-569-5.

Изложены базовые знания, необходимые для понимания цифровых технологий, внедряемых в нефтедобывающей отрасли, интеллектуализации нефтяных и газовых месторождений, технологии для повышения операционной эффективности. Также освещены вопросы кибербезопасности и операционного управления на объектах нефтедобывающей отрасли.

Для студентов, обучающихся по специальностям углубленного образования 7-06-0724-01 «Нефтегазовый инжиниринг» и непрерывного образования 7-07-0724-02 «Разработка и эксплуатация нефтяных и газовых месторождений».

Учебное пособие разработано и реализовано в рамках гранта Президента Республики Беларусь на 2025 год.

УДК 622.276:004(075.8)
ББК 33.3я73

ISBN 978-985-535-569-5

Оглавление

Предисловие 5
Глава 1. Цифровизация – концепция и определения 7
1.1. Основные понятия и определения цифровизации 7
1.2. Стратегии цифрового развития Республики Беларусь на 2026–2030 годы 13
1.3. Ключевые проблемы цифровой трансформации нефтегазовой отрасли 15
Глава 2. Цифровизация и автоматизация технологических процессов 27
2.1. Платформенные решения 27
2.2. Цифровые экосистемы 36
2.3. Цифровизация и автоматизация добычи газа и нефти 40
2.4. Использование цифрового двойника в нефтегазовой отрасли 47
2.5. Интеллектуальное (цифровое) месторождение: понятие и структура 51
2.6. Интегрированная модель месторождения 54
2.7. Мониторинг и управление механизированным фондом скважин 61
2.8. Цифровой двойник скважины с установкой погружных электроцентробежных насосов скважин как средство мониторинга текущей ситуации и прогноза оптимального режима 74
2.9. Роботизированная автоматизация 77
2.10. Внедрение беспилотных летательных аппаратов 81
Глава 3. Инструменты цифровой трансформации 86
3.1. Машинное зрение 86
3.2. Технологии работы с большими данными 90
3.3. Искусственный интеллект и машинное обучение 95
3.4. Система обучения по прецедентам 102
3.5. Облачные решения и системы. Облачные вычисления 105
3.6. Промышленный Интернет вещей (IIoT) 108
3.7. Инженерные симуляторы 125
3.8. Блокчейн в нефтегазовой отрасли 127
3.9. Операционная эффективность предприятия за счет цифровых инструментов SCADA, MES, ERP 128

Глава 4. Кибербезопасность и операционная эффективность ... 137
4.1. Нормативные документы по кибербезопасности Республики Беларусь ... 137
4.2. Общие понятия о кибербезопасности ... 140
4.3. Объекты защиты и задачи информационной безопасности в нефтегазовой отрасли ... 142
4.4. Методы обеспечения безопасности персональных компьютеров и Интернета, вирусы и антивирусы ... 145
4.5. Информационная безопасность вычислительных сетей ... 154
4.6. Комплексный подход к промышленной кибербезопасности ... 158
4.7. Мониторинг инцидентов кибербезопасности ... 161
4.8. Методы и средства защиты информации ... 165
4.9. Экосистемный подход к кибербезопасности предприятия ... 168
4.10. Тренды кибербезопасности 2025 года: анализ угроз и необходимые навыки специалистов ... 171
4.11. Риск-ориентированная модель информационной безопасности ... 174
Заключение ... 180
Литература ... 181

Предисловие

Цифровая трансформация производственных процессов нефтедобывающей отрасли охватывает все стадии разработки и эксплуатации современного месторождения углеводородов – от контрольно-управленческих функций до организации документооборота и планирования бизнес-процессов.

Тема цифровой трансформации остается в центре внимания не только профессионального ИТ-сообщества, но и большинства инженерных специалистов, которые должны иметь базовое представление о структуре и ключевых технологиях, определяющих развитие интеллектуальных месторождений. Цифровизация нефтегазовой отрасли в период с 2025 по 2030 г. будет расти в среднем на 17–20 % в год. Перечислим основные цифровые решения, которые используют в нефтегазовом секторе: цифровые двойники; искусственный интеллект; система обучения по прецедентам; облачные вычисления; умные материалы; роботизированная автоматизация; беспилотники; промышленный Интернет вещей (IoT); обработка большого массива данных; другие технологии и разработки.

Введение цифровых технологий позволяет улучшить контроль за производственными процессами, оптимизировать логистику, а также повысить безопасность и снизить воздействие на окружающую среду. Для успешного внедрения цифровых технологий в управлении нефтегазовыми комплексами необходимо не только использовать новые технологии, но и подготовить квалифицированных кадров, которые могут работать с этими технологиями. Кроме того, внедрение цифровых технологий требует соблюдения экологических и кибербезопасных требований, а также учета социальных и экономических аспектов. Именно эти вопросы будут рассматриваться в модуле «Цифровизация нефтегазовой отрасли», состоящем из двух дисциплин «Цифровая трансформация производственных процессов» и «Кибербезопасность и операционная эффективность».

Целями освоения модуля дисциплины является приобретение студентами специальности магистратуры 7-06-0724-01 «Нефтегазовый инжиниринг» теоретических и практических знаний в области цифровых технологий, используемых в нефтедобывающей отрасли, в частности, интеллектуализации нефтяных и газовых месторождений, формирование общих представлений о цифровой безопасности в ин-

формационном обществе, на объектах нефтедобывающей отрасли, а также умение применять правила кибербезопасности во всех сферах деятельности.

Предлагаемое учебное пособие является одной из попыток систематизировать знания и в доступной форме описать технологии, которые принято связывать сегодня с цифровизацией. Книга состоит из четырех глав, в которых цифровая трансформация нефтегазодобывающей отрасли рассмотрена в разных аспектах.

Учебное издание адресовано студентам, магистрантам и тем, кто хочет знать основные направления цифровой трансформации в нефтегазодобывающей отрасли на уровне концептуальных понятий, и понимать, как цифровые технологии меняют производственные процессы на уровне месторождений и предприятий.

Учебное пособие выполнено в рамках гранта Президента Республики Беларусь в сфере образования на 2025 г. (распоряжение № 15рп от 27 января 2025 г.), имеющего преимущественное значение для реализации государственных программ и важнейших направлений социально-экономического развития Республики Беларусь.

Автор выражает особую благодарность руководящему составу РУП «ПО «Белоруснефть» за помощь в проведении для учащихся экскурсий и занятий в структурных подразделениях, направленных на обучение цифровым и инновационным технологиям по специальностям «Нефтегазовый инжиниринг» и «Разработка и эксплуатация нефтяных и газовых месторождений».

Глава 1. ЦИФРОВИЗАЦИЯ – КОНЦЕПЦИЯ И ОПРЕДЕЛЕНИЯ

1.1. Основные понятия и определения цифровизации

В связи с наращиванием уровня и темпов цифровизации в Беларуси и во всем мире все больше предприятий стремятся осуществить перевод своих бизнес-процессов в цифровую среду, обеспечивая снижение издержек и увеличивая объемы экономической деятельности. Однако, несмотря на растущую популярность и распространение цифровизации на все сферы общества, данное понятие не имеет закрепленного определения в официальных нормативных документах. В связи с этим возникает ситуация, при которой основные термины, характеризующие цифровизацию, выступают в роли взаимозаменяемых понятий.

Информация лежит в основе современных цифровых технологий. Существует множество определений, однако ИТ-специалисты достаточно часто используют значение термина в узком смысле, поскольку, обрабатывая и анализируя данные (представляющие некоторую первичную информацию), могут выявлять скрытые закономерности, т. е. обнаруживать ранее неизвестную информацию. В этом случае данные – это исходный материал для обработки, в то время как информация – это продукт обработки, ее результат.

За последние несколько лет Беларусь и Россия увеличила темпы цифровизации по многочисленным направлениям, что позволяет странам развиваться и достигать лидирующих позиций в мире, следуя актуальным тенденциям. Собственные крупные технологические компании стран, которые успешно конкурируют с глобальными игроками на национальном и международном рынке, создают инфраструктурные инновации (от социальных сетей до беспилотных автомобилей) и оказывают серьезное технологическое влияние на рынок в целом [1].

Автоматизация, информатизация, цифровизация и, наконец, цифровая трансформация – это, по сути, последовательные этапы в развитии производственных процессов. Вначале происходила замена ручного труда машинным (автоматизация), в дальнейшем, с появлением средств вычислительной техники, они стали использоваться для

выполнения расчетов, а также управления оборудованием (информатизация). По мере развития цифровых технологий и широкого их распространения в сфере телекоммуникаций, а также развития интегрированных информационных систем и систем аналитики начался процесс цифровизации. Массовая цифровизация привела к появлению бизнес-моделей, полностью выстроенных на основе цифровых процессов, использование которых в различных областях человеческой деятельности стало качественно изменять структуру экономики. Этот процесс получил название цифровой трансформации.

Приведем кратко основные понятия и определения в контексте цифровой трансформации производственных процессов и кибербезопасности.

Информатизация – организационный, социально-экономический и научно-технический процесс, обеспечивающий условия для формирования и использования информационных ресурсов и реализации информационных отношений [2, 3].

Цифровизация – этап автоматизации и информатизации экономической деятельности и государственного управления, процесс перехода на цифровые технологии, в основе которого лежит использование для решения задач производства или управления информационно-коммуникационных технологий и накопление и анализ с их помощью больших данных в целях прогнозирования ситуации, оптимизации процессов и затрат, привлечения новых контрагентов и т. д. [4].

Оцифровка – это перевод процессов в digital-формат.

Цифровая трансформация – проявление качественных изменений, выраженных в принципиальном изменении структуры экономики, переносе центров создания добавленной стоимости в сферу выстраивания цифровых ресурсов и реализации сквозных цифровых процессов (эталонное нормативное определение).

Большие данные – обширные наборы данных, характеризующиеся значительными объемами, разнообразием, скоростью обработки и/или вариативностью, требующие масштабируемой технологии для эффективного хранения, манипулирования, управления и анализа [5].

Индустрия 4.0 (четвертая промышленная революция) – собирательное понятие, охватывающее ряд современных технологий, связанных с автоматизацией, обменом данных и производства. Понятие определено как набор технологий и концепций для организации цепи создания стоимости, включающий облачные технологии, искусственный интеллект (ИИ), Интернет вещей, большие данные, виртуальную

и дополненную реальность, блокчейн и т. п. Главное отличие технологий Индустрии 4.0 от предыдущих состоит в том, что они соединяют устройства между собой с целью обмена данными и решения производственных задач без участия человека.

Интернет вещей (IoT) – это сеть связанных через Интернет объектов, способных собирать данные и обмениваться данными, поступающими со встроенных сервисов. Устройства, входящие в IoT, могут отслеживаться и/или управляться удаленно.

Информационная инфраструктура:

– совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации;

– совокупность информационных систем и организационных структур, обеспечивающих функционирование и развитие информационного пространства страны и средств информационного взаимодействия.

Информационная система:

– совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств;

– организованная совокупность информационных технологий, объектов и отношений между ними, образующая единое целое. Информационная система может включать в качестве объектов персонал, информационные, материально-технические и другие ресурсы, необходимые для реализации конкретного информационного процесса.

Информационная технология – совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации.

Информационно-коммуникационная инфраструктура – совокупность сетей электросвязи и информационных сетей, оконечных устройств, информационных ресурсов, которые могут быть использованы для получения доступа к той или иной информации и организации связи между пользователями в любое время и в любом месте, по доступной цене.

Информационно-коммуникационные технологии (ИКТ) – совокупность информационных технологий и технологий электросвязи, обеспечивающих сбор, обработку, хранение, распространение, отображение и использование информации в интересах ее пользователей.

Информационное общество – общество, в котором информационные процессы осуществляются на основе использования информационно-коммуникационных технологий, а информационные ресурсы

доступны членам общества и направлены на удовлетворение их потребностей в информационных услугах и информационной продукции.

Информационное пространство:

– область деятельности, связанная с созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие в том числе на индивидуальное и общественное сознание и собственно информацию;

– совокупность информационных ресурсов, информационных систем и коммуникационной среды.

Искусственный интеллект (AI) – это система или машина, которая может имитировать человеческое поведение, чтобы выполнять задачи, и постепенно обучаться, используя собираемую информацию. AI имеет множество воплощений:

– чат-боты используют AI, чтобы анализировать обращения заказчиков и давать соответствующие ответы;

– «умные помощники» используют AI, чтобы извлекать информацию из больших наборов данных в произвольной форме и оптимизировать планирование;

– системы рекомендаций автоматически подбирают похожие программы для телезрителей на основе ранее просмотренных.

Машинное обучение – класс методов ИИ, характерной чертой которых является не прямое решение задачи, а обучение в процессе применения решений множества сходных задач.

Облачное хранилище – модель онлайн-хранилища, в котором данные хранятся на многочисленных распределенных в сети серверах, предоставляемых в пользование клиентам, в основном третьей стороной. В отличие от модели хранения данных на собственных выделенных серверах, приобретаемых или арендуемых специально для подобных целей, количество или какая-либо внутренняя структура серверов клиенту в общем случае не видна. Данные хранятся и обрабатываются в так называемом «облаке», которое представляет собой, с точки зрения клиента, один большой виртуальный сервер. Физически такие серверы могут располагаться удаленно друг от друга географически.

Промышленный Интернет вещей, *индустриальный Интернет вещей, индустриальный Интернет* – концепция построения инфокоммуникационных инфраструктур, подразумевающая подключение к сети Интернет любых небытовых устройств, оборудования, датчиков, сенсоров, автоматизированной системы управления технологиче-

ским процессом, а также интеграцию данных элементов между собой, что приводит к формированию новых бизнес-моделей при создании товаров и услуг, а также их доставке потребителям.

Средства электронной цифровой подписи – программные и технические средства, обеспечивающие выработку и проверку электронной цифровой подписи и имеющие сертификат соответствия или удостоверение о признании сертификата, выданного в Национальной системе подтверждения соответствия Республики Беларусь.

Стратегия цифровой трансформации – интегрированная модель действий в бизнесе (национальной политике), предназначенных для достижения целей предприятия (государства), нацеленных на выполнение стратегических задач цифрового преобразования экономики.

Цифровая инфраструктура – комплекс технологий и построенных на их основе цифровых продуктов, обеспечивающих вычислительные, телекоммуникационные и сетевые мощности и работающих на цифровой основе.

Цифровая культура – понимание современных информационных (цифровых) технологий, их функциональных возможностей, а также возможность грамотно использовать их в работе или в быту.

Цифровая стратегия – маркетинговый план, цель которого заключается в общем развитии и преобразовании бизнеса, популяризации продукта или бренда; на национальном уровне – всеобъемлющая государственная программа преобразований (цифровой трансформации) во всех аспектах экономики и жизни общества на основе передовых достижений науки и производства.

Цифровая технология – технология, в отличие от аналоговой, работающая с дискретными, а не с непрерывными сигналами.

Цифровая экономика – часть экономики, в которой процессы производства, распределения, обмена и потребления прошли цифровые преобразования с использованием информационно-коммуникационных технологий.

Цифровое пространство – пространство, интегрирующее цифровые процессы, средства цифрового взаимодействия, информационные ресурсы, а также совокупность цифровых инфраструктур на основе норм регулирования, механизмов организации, управления и использования.

Цифровой двойник – виртуальная цифровая модель (прототип) существующего в реальности физического объекта или процесса, моделирующая внутренние процессы, технические характеристики и

поведение реального объекта в условиях взаимодействия помех и окружающей среды.

Цифровой след – совокупность информации о посещениях и вкладе пользователя во время пребывания в цифровом пространстве.

Цифровые инновации – новое средство, использующее цифровые процессы, ресурсы и сервисы на основе технологий больших данных, нейротехнологий и ИИ, системы распределенного реестра (блокчейн), квантовых технологий, новых производственных технологий, промышленного интернета, компонентов робототехники и сенсорики, технологий беспроводной связи, виртуальной и дополненной реальностей и других технологий, которые в государственных правовых актах отражены как относящиеся к цифровым или к цифровой экономике; новая система таких средств или новая форма использования такого существующего средства/системы средств.

Цифровые навыки – компетенции населения в области применения персональных компьютеров, Интернета и других видов информационно-коммуникационных технологий, а также намерения людей в приобретении соответствующих знаний и опыта.

Экономика данных – результат формирования больших объемов данных с помощью технических устройств и других источников, обмена ими и накопления для последующего анализа, принятия решений и формирования новой добавленной стоимости.

Защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

Информационный потенциал – совокупность средств, методов и условий, позволяющих использовать информационные ресурсы.

Информационный ресурс:

– совокупность информации, содержащейся в различных источниках;

– организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах.

Кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации

взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

Кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз.

Кибертерроризм – атаки на информационные системы, несущие угрозу здоровью и жизни людей, способные спровоцировать серьезные нарушения функционирования критически важных объектов в целях оказания воздействия на принятие решений органами власти либо воспрепятствования политической или иной общественной деятельности, либо устрашения населения, либо дестабилизации общественного порядка.

Персональные данные – основные и дополнительные персональные данные физического лица, подлежащие в соответствии с законодательными актами Республики Беларусь внесению в регистр населения, а также иные данные, позволяющие идентифицировать такое лицо [2].

Интернет – совокупность взаимосвязанных международных сетей передачи данных, основанных на использовании стека протоколов TCP/IP и использующих единое адресное пространство [3].

1.2. Стратегии цифрового развития Республики Беларусь на 2026–2030 годы

Цели и задачи госполитики в сфере цифрового развития строятся на определенных принципах, среди которых: принцип эффективного планирования цифрового развития на всех уровнях государственного управления; принцип обеспечения технологического и цифрового суверенитета; принцип признания данных в качестве ключевого стратегического актива государства; принцип установления в качестве приоритетов развития электронного правительства; принцип масштабирования уже существующих успешных практик на различные области государственной деятельности.

Государственная программа «Цифровое развитие Беларуси» на 2021–2025 гг. (https://www.mpt.gov.by/ru/gosudarstvennaya-programma-cifrovoe-razvitie-belarusi-na-2021-2025-gody) разработана в соответствии с приоритетными направлениями социально-экономического развития республики до 2025 г. и направлена на внедрение ин-

формационно-коммуникационных и передовых производственных технологий в отрасли национальной экономики и сферы жизнедеятельности общества.

С целью дальнейшего цифрового развития страны, последовательной цифровой трансформации экономической деятельности и государственного управления, а также обеспечения цифрового лидерства в Беларуси утвердили Стратегии цифрового развития Республики Беларусь на 2026–2030 гг. и на период до 2035 г. (приказ Министерства связи и информатизации от 23.05.2025 г. № 108). В основу легли комплексные аналитические материалы, которые дают всестороннее понимание текущего состояния цифровизации, а также глобальных трендов и вызовов.

На основании оценки уровня цифрового развития практически всех предприятий, подчиненных государству, сформированы долгосрочные цели развития на 2026–2030 гг. и прогнозные показатели в Стратегии цифрового развития Республики Беларусь, которая будет затрагивать три уровня: регулятор цифрового развития, отраслевую экономику (регионы), отдельные организации. Основными стратегическими направлениями определены: цифровые услуги, данные и уход от ручного управления к предикативному. Также в рамках Стратегии будут выстроены механизмы условий цифрового развития, порядок взаимодействия и инструменты для реализации данной стратегии, предложен приоритетный сценарий цифрового взаимодействия и др.

Основные аналитические выводы и глобальные тенденции, учтенные в стратегии

Мировая практика цифровых стратегий. В 2023 г. 90 % стран мира имели или разрабатывали национальную цифровую стратегию, а треть из 1200 политических инициатив ОЭСР направлена на стимулирование цифровых технологий.

Рост инвестиций в ИИ. Глобальные венчурные инвестиции в стартапы в сфере ИИ утроились с 2015 по 2023 г., достигнув 98 млрд долл. США.

Экономика данных. Ежедневно в 2024 г. генерируется 2,5 квинтиллиона байт данных, при этом 90 % мировых данных были созданы за последние два года и 80 % промышленных данных, по оценке ЕС, остаются неиспользованными.

Влияние цифровой общественной инфраструктуры (DPI). Исследования показывают, что DPI может ускорить рост совокупного ВВП стран с низким и средним уровнем дохода на 19,2 трлн долл.

США к 2030 г. Например, в Индии цифровые платежные системы, являющиеся частью DPI, ежемесячно обрабатывают 13 млрд транзакций, что позволило правительству сэкономить 41 млрд долл. США.

Эффективность электронного правительства. Внедрение клиентоцентричных принципов в госуправлении в России привело к сокращению на 662 единицы количества необходимых документов, на 5225 дней – сроков ожидания услуг, и на 679 – количества контактов с госорганами. В Казахстане уже 90 % госуслуг предоставляется в электронном формате, с целью достигнуть 100%-ной цифровизации услуг, оказываемых за 5 минут, к 2029 г.

Рост ИТ-сектора. Инвестиции в технологии приводят к трансформации отраслей беспрецедентными темпами. Ускорение положительной динамики объясняется несколькими факторами: увеличение расходов на программное обеспечение и ИТ-услуги, включая генеративный искусственный интеллект (ГенИИ), облачные платформы, решения для обеспечения информационной безопасности, цифровые технологии и кибербезопасность. Эти направления займут центральное место на ИТ-рынке, преобразуя работу компаний. Организации, которые отдают приоритет этим направлениям, не только укрепят свои конкурентные преимущества, но и добьются устойчивого роста.

Эти и другие аналитические данные подчеркивают важность цифровой трансформации для устойчивого развития страны, повышения качества жизни граждан и конкурентоспособности бизнеса в цифровую эпоху.

1.3. Ключевые проблемы цифровой трансформации нефтегазовой отрасли

Современная нефтегазовая промышленность по показателям глубины цифровой зрелости занимает 14-е место из 18-ти в отчете Массачусетского технологического института, уступая предприятиям телекоммуникации, СМИ и розничной торговли. Цифровая трансформация предприятий нефтегазовой отрасли является одним из важнейших компонентов сохранения конкурентоспособности на мировом рынке и они вкладывают большие инвестиции в реализацию своих технологических стратегий цифровых преобразований.

Стратегирование – это совокупность процессов планирования, прогнозирования и управления; формирование будущего с опорой на многоаспектное описание существующей реальности, знания о законах изменений и способность реагировать на меняющуюся реальность.

Разработка методологии стратегирования цифровой трансформации предприятий нефтегазовой отрасли является важной из-за ряда условий:

– современная общемировая ситуация и изменение цен на газ и нефть из-за санкционной политики в отношении России;

– необходимость в разработке трудноизвлекаемых запасов нефти и газа с использованием цифровых моделей;

– рост конкурентоспособности: на базе внедрения цифровых технологий оптимизируются все бизнес-процессы (основные, вспомогательные и обслуживающие развитие) и снижаются затраты;

– усложнение требований к безопасности и рост экологических требований: деятельность предприятий нефтегазовой отрасли сопряжена с рисками, связанными с авариями и утечками нефти и газа. Цифровые системы мониторинга и управления оперативно обнаруживают и реагируют на потенциально опасные ситуации, что способствует решению проблем безопасности;

– цифровизация позволяет быстрее адаптироваться к новым технологическим трендам, таким как «цифровые месторождения», «аддитивные технологии» и «умные» сети;

– универсализация процессов обслуживания клиентов.

Развитие организационно-экономического механизма стратегирования цифровой трансформации нефтегазовых предприятий связано с выработкой определенного подхода к этому процессу. Все существующие подходы представлены в табл. 1.1.

Мы придерживаемся синергетического подхода, объединяющего все перечисленные направления трансформации в процессах стратегирования.

Таблица 1.1

Подходы к стратегированию цифровой трансформации предприятия

Подход	Суть подхода
Пользовательско-центричный	Основан на удовлетворении потребностей и ожиданий клиентов. Организации анализируют данные о своих клиентах, чтобы создать персонализированные цифровые решения
Инновационный	Базируется на создании конкурентных преимуществ через новаторские технологии и решения. Организации инвестируют в исследования и разработки, чтобы быть лидерами в своей отрасли

Окончание табл. 1.1

Подход	Суть подхода
Agile-подход	Предполагает быструю реакцию на изменения и адаптацию к рыночным требованиям. Организации используют методики Scrum и Kanban для управления проектами и разработки продуктов. Стратегические решения тестируются сразу после разработки, параллельно внедряются цифровые технологии. Такой подход может обеспечить положительный эффект еще до завершения всего процесса
Экосистемный	Фокусируется на участии в экосистемах и создании партнерских отношений. Организации стремятся взаимодействовать с другими субъектами бизнес-среды, чтобы совместно создавать ценность для клиентов
Синергетический	Объединяет все перечисленные направления трансформации в процессах стратегирования

Выбор конкретного подхода и модели стратегирования цифровой трансформации зависит от поставленной цели, задач, особенностей внутренней среды организации, внешних рыночных условий и специфики отрасли, в которой она работает.

Цифровизация нефтегазовых предприятий имеет несколько ключевых особенностей:

1. *Сбор и анализ данных*: цифровизация обеспечивает сбор больших объемов данных с различных устройств и оборудования, таких как датчики, мониторы и счетчики. Анализ таких данных помогает оптимизировать процессы и улучшить предсказуемость операций.

2. *Управление активами*: цифровые технологии выполняют функции отслеживания состояния и производительности газопроводов, компрессорных станций и другого оборудования. Это способствует более эффективному управлению активами и увеличению срока службы оборудования.

3. *Безопасность*: цифровизация повышает качество процессов мониторинга и контроля за безопасностью в газовой отрасли. Системы управления безопасностью и детекторы аварий связаны с центральными системами для оперативного реагирования на потенциальные угрозы.

4. *Оптимизация процессов*: автоматизация и оптимизация процессов в добыче, транспортировке и распределении газа и нефти позволяют снижать затраты и повышать производительность.

5. *Экологические аспекты*: цифровизация помогает улучшить экологическую устойчивость нефтегазовой промышленности через мониторинг выбросов и оптимизацию процессов снижения негативного воздействия на окружающую среду.

6. *Инновации*: цифровизация способствует развитию новых технологий, таких как «умные сети», для распределения газа и нефти, использованию ИИ для анализа данных и более эффективного управления ресурсами.

7. Внедрение цифровых технологий оптимизирует процессы обслуживания клиентов.

В рамках стратегирования цифровой трансформации нефтегазовых предприятий необходимо провести OTSW-анализ (возможности, угрозы, сильные и слабые стороны). Согласно концепции стратегирования В. Л. Квинта, «OTSW-анализ (Opportunities, Threats, Strengths, Weaknesses) намного точнее соответствует процессу формирования стратегического видения, приоритетов объекта, так как более эффективно подготавливает компании, регионы и страны к неожиданно возникающим возможностям или угрозам», также он позволяет более эффективно подготовиться к возникающим возможностям или угрозам и получить преимущество во времени.

Предложенный В. Л. Квинтом порядок направлен на выявление возможностей, реализация которых может быстро закрыться.

Затем анализируются *угрозы* и *сильные стороны*, потом *слабые* стороны объекта анализа, так как они могут быть усилены.

Ключевые возможности (Opportunities) стратегирования цифровой трансформации нефтегазовых предприятий:

– использование развивающейся нормативно-правовой базы для реализации возможностей применения цифровых технологий;

– стандартизация отраслевых данных для формирования единого информационного пространства;

– активизация процессов цифровизации на базе более широкого применения финансовых и нефинансовых мер, связанных с совершенствованием регуляторных условий апробации, стандартизации и сертификации отечественных цифровых разработок;

– накопление цифрового опыта и создание банков успешных практик;

– расширение возможностей использования цифровых технологий в процессах взаимодействия между органами власти и компаниями;

– рост эффективности добычи и распределения газа и нефти с использованием IoT-технологий;

– разработка новых бизнес-моделей, таких как предоставление услуг «умных домов» и «умных городов».

В качестве *основных угроз* (Threats) можно выделить:

– недостаток квалифицированных кадров, способных работать с новыми технологиями;

– отсутствие в новых регионах освоения углеводородов необходимой инфраструктуры;

– ограничения технологического сотрудничества и уход с отечественного рынка мировых лидеров нефтесервиса [49];

– недостаток сопоставимых с западными технологиями отечественных цифровых разработок и отсутствие их правовой защиты на фоне требований к импортозамещению;

– неготовность сложившейся институциональной среды к внедрению сквозных платформенных цифровых решений и формированию единого цифрового пространства.

Сильными сторонами (Strengths) предприятий нефтегазовой отрасли являются:

– глобальное территориальное присутствие;

– функционирование в виде четко выстроенных интегрированных вертикальных структур;

– сильный бренд и надежная репутация;

– практически все нефтегазовые компании опираются в своей работе на проект «Цифровая энергетика» в рамках реализации государственной программы «Цифровая экономика»;

– достигнутая устойчивая динамика повышения точности прогнозов спроса и снижения издержек в цепи поставок благодаря аналитике данных;

– развитие «умных» сетей с возможностью удаленного управления и мониторинга;

– создание и развитие отраслевых центров компетенций и корпоративных университетов, подготовка новых образовательных программ цифровой грамотности отраслевыми вузами для нужд предприятий ТЭК;

– активный поиск и апробация предприятиями систем показателей глубины и эффективности внедрения цифровых технологий.

Слабыми сторонами (Weaknesses) можно считать:

– недостаточные суммы денежных средств на внедрение цифровых систем и обучение персонала;

– необходимость в защите критических информационных систем от кибератак;

– недостаточное количество формализованных и гибких методик стратегирования цифровой трансформации предприятий.

Стратегирование направлено на реализацию выявленных возможностей развития, которые основаны на глобальных, национальных, региональных и отраслевых трендах. Отечественные и зарубежные нефтегазодобывающие компании успешно реализуют цифровые проекты. Приведем некоторые примеры.

Республиканское унитарное предприятие «Производственное объединение «Белоруснефть» – государственная вертикально-интегрированная нефтяная компания, реализует проекты по освоению нефтегазовых ресурсов не только в Беларуси, но и в странах ближнего и дальнего зарубежья в партнерстве с крупнейшими энергетическими корпорациями мира. Цифровая трансформация становится новым драйвером развития «Белоруснефти». Специалисты компании выстраивают интегрированную цепочку: «цифровое месторождение», «цифровое бурение», «цифровой завод», «цифровая энергетика», «цифровая геологоразведка».

Ключевая задача компании – концептуальное проектирование. Каждый бизнес-процесс стал проектным решением, где уже было определено программное обеспечение. Разработана концепция и схема интеграции между всеми процессами. В концепт включены новые и уже имеющиеся в «Белоруснефти» программные продукты. Большая работа проделана по доработке базы данных Oraview. Итогом стала разработка интеллектуальной системы по контролю за работой фонда скважин и технологических объектов, формированию интегрированного плана работы промысла, ведению производственного учета добычи, техобслуживания и ремонта оборудования, автоподбора геолого-технологических мероприятий.

Цифровой актив предприятия складывается из следующих составляющих: Центра интегрированных операций НГДУ «Речицанефть», который в режиме реального времени следит за всем происходящим на объектах нефтедобычи с использованием системы телеметрии, мгновенно реагирует на любые изменения и отклонения от заданных параметров.

В перспективе расширение интеллектуальной системы «Цифровое месторождение» планируется в цехе подготовки и перекачки нефти для более качественного контроля за эксплуатацией оборудования, планирования его техобслуживания и ремонта. Начато внедрение системы «Цифровая платформа строительства скважин». Она оптимизи-

рует график бурения новых скважин, логистику передвижения станков, усилит контроль за сроками разработки и выдачи проектно-сметной документации, строительства и обустройства инфраструктуры. На БГПЗ идут работы по концептуальному проектированию системы «Цифровой завод». Основные задачи: моделирование динамики технологических процессов, формирование и анализ выполнения планов производства, формирование материальных балансов и технологического режима. На стадии концептуального проектирования «Цифровая энергетика», предусматривающая создание единой системы мониторинга работы всей энергетической инфраструктуры предприятия. В блоке геологоразведки идет поиск цифрового решения, учитывающего все наработки «Белоруснефти» в полевой и камеральной сейсморазведке, керновых исследованиях, создании геологических моделей месторождений. Интеграция цифровых платформ в единое информационное поле позволит компании «Белоруснефть» более качественно выстраивать планы развития, нацеленные на увеличение добычи нефти.

ПАО «Газпром» (Россия) активно внедряет цифровые технологии, включая системы мониторинга и управления газопроводами, автоматизацию процессов добычи и транспортировки газа. Начиная с 2019 г. запустило на своих площадках более 150 новых цифровых инициатив и более десятка программ цифровой трансформации. С 2022 по 2026 г. реализуются мероприятия, принятые в Стратегии цифровой трансформации Группы «Газпром», которая разработана в соответствии с методическими рекомендациями Министерства цифрового развития, связи и массовых коммуникаций РФ.

Группой разработана и утверждена стратегия цифровой трансформации до 2030 г. **ПАО «НОВАТЭК» (Россия)** использует цифровизацию в своих проектах по добыче и переработке природного газа. НОВАТЭК НТЦ заменил агрегацию информации из суточных отчетов супервайзеров в единый формат и рассылку информации по электронной почте на технологию виртуального ассистента, позволяющую сотруднику получать ответы на заданные вопросы помощнику за несколько секунд без подключения к Интернету.

Sinopec (Китай) активно использует технологии и услуги для цифровой нефтегазовой индустрии, включая мониторинг скважин и аналитику данных. China National Petroleum/PetroChina (Китай) предоставляет и использует решения для автоматизации и цифровизации, активно развивает цифровые решения для улучшения эффективности добычи и транспортировки газа и нефти.

Цифровой портфель предприятий нефтегазовой сферы включает технологию «умные материалы», «когнитивную геологию», современные технологии мониторинга и цифрового прототипирования, роботизацию и «безлюдные технологии», 3D- и 4D-моделирование, анализ больших данных, блокчейн, облачные вычисления, Интернет вещей, цифровые двойники, ИИ и машинное обучение.

Анализируя отраслевую специфику, необходимо отметить, что из всех цифровых технологий лидирующие позиции занимает промышленный Интернет вещей – 22 % (рис. 1.1).

Рис. 1.1. Цифровые тренды Индустрии 4.0 в нефтегазовой отрасли в мире в 2024 г.

Наиболее зрелыми областями стратегирования цифровой трансформации для предприятий нефтегазовой отрасли являются инновации, операционная деятельность и цепочки поставок, а процессы стратегирования рисков и кибербезопасности требуют проработки стратегических и операционных планов компании. Эти направления цифровой трансформации важно включать в число стратегических приоритетов нефтегазовых организаций в процессах формализации стратегий цифровой трансформации.

Менеджмент нефтегазовых предприятий ищет стратегические резервы роста конкурентоспособности и способы увеличения прибыльности за счет снижения затрат и встраивания в бизнес-процессы новых цифровых технологий и профессиональных навыков.

На следующем этапе стратегирования разрабатывают миссию и видение.

Миссия стратегирования цифровой трансформации нефтегазовых предприятий состоит в масштабировании сетевой логики взаимодействия всех заинтересованных участников, ускоряющем создание и развитие кроссфункциональных экосистем, для осуществления безбарьерного трансферта знаний, технологий и компетенций.

Под *видением* будет пониматься создание условий для реализации указанной миссии. Видение основано на гармоничном функционировании и соразмерной динамичной эволюции элементов, структур и процессов стратегирования.

Миссия и *видение* являются базой для постановки цели и формулирования задач стратегирования цифровой трансформации предприятий нефтегазовой промышленности, которая заключается в проведении цифровых преобразований в действующих бизнес-моделях на всех стадиях создания добавленной стоимости.

Задачами цифровой трансформации нефтегазовых предприятий являются:

– качественное повышение уровня гибкости и адаптивности существующих бизнес-моделей предприятий нефтегазовой отрасли;

– платформизация бизнес-процессов, которая предусматривает использование цифровых торговых платформ, смарт-контрактов и цифровых финансовых активов;

– повышение качества стратегирования на уровне предприятия, направленного на совершенствование корпоративной культуры и реализацию структурных изменений.

Решение задач создаст основу для осмысления стратегии цифровой трансформации предприятия, которая включает этапы, взаимоувязанные по срокам, исполнителям и предполагаемым результатам (табл. 1.2).

Таблица 1.2

Модель стратегии цифровой трансформации предприятия

Этапы формирования стратегии	**«Узкие места»**	**Ответственные лица**	**Результаты этапа**
Анализ текущего состояния предприятия, оценка технологических систем, процессов и инфраструктуры	Недостаточно данных для полного анализа, недооценка сложности существующей инфраструктуры	Члены аналитической группы	Составление отчета о текущем состоянии инфраструктуры, идентифицированы основные технологические слабые места

Окончание табл. 1.2

Этапы формирования стратегии	**«Узкие места»**	**Ответственные лица**	**Результаты этапа**
Определение стратегических целей и задач, разработка видения достижения целей	Несогласованность цифровой стратегии с общей стратегией предприятия	Топ-менеджмент, стратегический отдел	Стратегическая цель цифровизации, ключевые задачи для достижения цели
Идентификация цифровых решений: выбор технологий, программного обеспечения и систем	Недостаточный бюджет на приобретение необходимых технологий, сложности в интеграции выбранных решений	ИТ-отдел, технические специалисты	Список потенциальных цифровых решений, оптимальных технологий и систем
Разработка плана внедрения	Недостаточные ресурсы для выполнения плана	Проектный менеджер, отдел планирования	Детальный план и сроки внедрения цифровых решений
Выделение ресурсов: бюджета, персонала и других ресурсов	Ограниченный бюджет для цифровизации, трудности в найме и обучении персонала	Финансовый отдел, HR-отдел	Бюджет цифровизации, необходимый кадровый ресурс
Внедрение цифровых решений	Технические проблемы, сопротивление персонала переменам	ИТ-отдел, проектная группа	Внедренные цифровые решения

Цифровизация промышленного комплекса включает полный анализ системы производства, бизнес-процессов, логистической поддержки и внешних факторов для определения стратегических мероприятий трансформации. Грамотная комплексная модернизация технологической цепочки большой компании осуществляется в несколько этапов:

– оценка цифровой зрелости предприятия;

– определение ряда мероприятий по оптимизации и повышению эффективности цифровой бизнес-архитектуры предприятия;

– цифровизация и автоматизация бизнес-процессов, диагностика и оптимизация существующей модели предприятия.

Следует отметить, что комплексная цифровая трансформация бизнес-процессов ведет к существенному увеличению объемов про-

изводства и, следовательно, прибыли, а также к повышению его конкурентоспособности и общей рыночной стоимости.

Для первоочередной реализации выделены 12 приоритетных программ цифровой трансформации в нефтедобывающей отрасли (рис. 1.2).

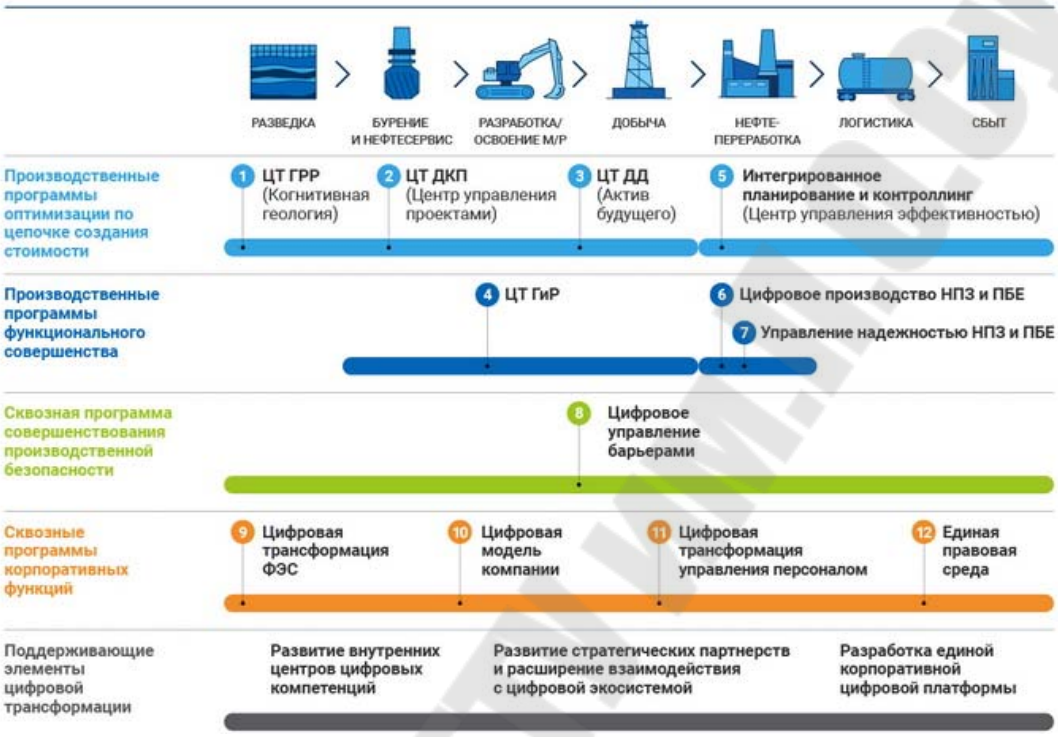

Рис. 1.2. Основные направления цифровой трансформации нефтедобывающей отрасли

Первый этап – аудит бизнес-процессов организации и анализ цифровой развитости предприятия.

Второй этап – непосредственно комплексная автоматизация производственного процесса. Цифровизация деятельности заключается в создании интеллектуального производства.

Концепция четвертой промышленной революции базируется на четырех принципах:

– функциональной совместимости человека и машины – возможности контактировать напрямую через Интернет;

– прозрачности информации и способности систем создавать виртуальную копию физического мира;

– технической помощи машин человеку – объединения больших объемов данных и выполнения ряда небезопасных для человека задач;

– способности систем самостоятельно и автономно принимать решения.

Выделяют следующие основные направления создания стоимости с помощью применения индустрии 4.0 в процессе производства:

– оптимизация режимов работы оборудования на основе анализа данных и управления технологическими процессами, осуществляемыми в онлайн-режиме;

– оптимизация загрузки оборудования, которая позволяет увеличить техническую готовность оборудования путем сокращения простоев, достигаемого с помощью планово-предупредительного подхода к ремонту и обслуживанию используемого оборудования;

– повышение безопасности и производительности труда позволит работникам различной квалификации более эффективно выполнять работу при помощи цифровизации;

– повышение качества производимой продукции с помощью цифровизации используемого оборудования и внедрения новых технологий и т. п.

Огромное влияние цифровые технологии оказывают на безопасность производства и охрану труда промышленного предприятия. Прежде всего это касается возможности размещения датчиков на эксплуатируемом оборудовании и персонале для автоматизированного мониторинга их перемещений по производственной площадке, анализа потенциально опасных действий, предотвращения травматизма и несчастных случаев на производстве [1].

Таким образом, цифровизация нефтедобывающей отрасли – это концепция нового цифрового пространства, единой системы, в которую интегрируются производственные составляющие.

Глава 2. ЦИФРОВИЗАЦИЯ И АВТОМАТИЗАЦИЯ ТЕХНОЛОГИЧЕСКИХ ПРОЦЕССОВ

2.1. Платформенные решения

Эффективное управление современными комплексными месторождениями углеводородов в целом невозможно без создания и внедрения современных цифровых систем и технологий, которые помогают повысить уровень управляемости развитием комплекса разработки и эксплуатации нефтяных и газовых месторождений в целом.

Цифровая трансформация подразумевает внедрение отраслевых платформенных решений и цифровизации взаимодействия с субъектами топливно-энергетического комплекса страны.

Информационную инфраструктуру в целом можно рассматривать как комплекс взаимосвязанных программно-аппаратных средств организации, которые направлены на обеспечение ее деятельности, а также являются фундаментом для осуществления процессов цифровизации и цифровой трансформации.

Цифровая трансформация осуществляется в том числе посредством включения платформенных решений и цифровых технологий в производственные процессы организаций.

Однако понятие «платформенное решение» не определено на государственном уровне, вместо этого существует множество интерпретаций и подходов, рассматривающих данное явление.

Платформенное решение – автоматизированная информационная система, доступ к которой обеспечивается посредством сети Интернет, позволяющая участникам данной системы решать свои технологические и функциональные задачи, благодаря чему возможно снижение транзакционных издержек и значительное увеличение производительности труда.

В настоящее время используется большое количество информационных систем, построенных с применением различных архитектурных решений, имеющих множество классов. Рассмотрим подробнее наиболее популярные классы информационных систем, выделенных на основе доменного подхода:

– управляющие системы;

– информационно-управляющие системы;

– системы управления доступом;

– системы мониторинга и управления ресурсами;

– системы управления производством.

Управляющие системы представляют собой комплекс технологических инструментов, описывающих бизнес-процесс (например, производственный) на предмет соответствия эталонным значениям и осуществляющих выдачу управляющего воздействия.

Информационно-управляющие системы осуществляют сбор, обработку, интерпретацию и предоставление в виде отчетности данных различным категориям пользователей для принятия решения на их основе.

Системы управления доступом направлены на обеспечение доступа субъектов к объектам и ресурсам в соответствии с определенными регламентными процедурами.

Системы мониторинга и управления ресурсами применяются для решения типовых для многих организаций задач, потоковых работ, таких как регистрация информации, отслеживание ее изменений, получение, отправка или уничтожение в виртуальном или реальном мире.

Системы управления производством имеют существенную отличительную особенность: на входе в технологическом процессе поступает сырье, а на выходе получается готовый продукт – объект физического или информационного мира.

Каждый из рассмотренных классов систем в зависимости от степени трансформации процессов, области и масштаба применения системы используется для автоматизации, цифровизации и цифровой трансформации.

Рассмотрим *системы управления производством* (СУП) – единственный из представленных классов, непосредственно осуществляющий вклад в создание добавленной стоимости конечной продукции, соответственно, существенно оказывающий влияние на процесс цифровой трансформации, повышение производительности труда и сокращение издержек.

СУП включает в себя четыре основных аспекта [14]:

– материальные потоки (трансформация материалов и сырья в готовый продукт);

– информационные потоки (планирование и управление производственными процессами);

– поток стоимости (финансовый аспект);

– организационные потоки (кадровый состав).

Материальные потоки задействуют ресурсы (капитал, сырье, труд) для создания готовой продукции. В рамках этого аспекта можно выделить основной процесс, который соединяет входы и выходы системы. Аспект включает в себя следующие активности, например, для нефтедобывающей отрасли: добыча углеводородного сырья; переработка; поставка на рынок; продажа.

Информационный поток отвечает за планирование производственных процессов и управление ими.

Поток стоимости определяет изменение цены произведенной продукции на каждой стадии технологического процесса.

Организационные потоки направлены на адаптацию кадров в условиях трансформационных процессов, развитие организационной зрелости и политики управления знаниями.

Общая практическая задача СУП, как и всей ИТ-инфраструктуры, заключается в обеспечении максимально эффективного и дешевого применения всех ресурсов системы и точного выполнения поставленного плана. Примером цифрового решения, являющегося частью ИТ-инфраструктуры, выступают цифровые двойники. Это одна из инновационных технологий, которая активно внедряется в процесс нефтедобычи и переработки.

Цифровые двойники – это математические модели, создаваемые для визуализации технологических и физических установок нефтеперерабатывающего завода (НПЗ). Они обязательно содержат информацию о характеристиках инженерных систем, средствах автоматизации, их сроках службы и периодах обслуживания, описание физико-химических процессов и процессов потребления и выработки энергии. В результате цифровые двойники фактически позволяют объединить существующую инфраструктуру в одну взаимосвязанную систему и синхронизировать работу всех ее частей.

Базой для цифровых двойников выступают информационные системы, которые проектируются для оптимизации производственных процессов и создания дополнительных источников статистических данных. Последние используются в аналитической части деятельности предприятия. Основными функциональными частями информационной системы (ИС) являются:

– сбор, хранение и обработка данных;

– представление данных в удобном виде в зависимости от назначения;

– формирование структуры взаимосвязи данных.

Главные части информационных систем:

– база данных, представляющая совокупность взаимосвязанных и упорядоченных данных;

– программные модули, отвечающие за обработку данных;

– пользовательский интерфейс для работы с информационной системой.

Информационные системы можно классифицировать по степени интеграции: локальные, малые интегрированные, средне интегрированные, крупно интегрированные.

Стремительный рост объема и источников данных вынуждает бизнес серьезно заниматься аналитикой. Первый шаг в этом направлении – централизация компетенций по сбору и первичной обработке важной информации в рамках специализированного подразделения внутри компании. Самым эффективным инструментом тут выступает Центр управления производством (ЦУП). Этапы развития платформы и решений представлены на рис. 2.1.

Рис. 2.1. Этапы развития платформы и решений ЦУП (www.nefteavtomatika.ru)

ЦУПы – современный цифровой тренд, который развивает вектор на централизацию управления данными компании. Формат ЦУПа близок традиционным диспетчерским, ситуационным центрам, но выходит за их рамки за счет более глубокой работы с собираемыми данными в исторической перспективе и через задачи прогнозирования.

ЦУП дает возможность избавиться от дублирования управленческих функций, помогает сформировать экспертные команды по бизнес-направлениям и является точкой запуска изменений в масштабах компании.

Современные ЦУПы можно разбить на четыре основных типа.

Базовая диспетчерская – помогает повысить прозрачность и наблюдаемость производственных процессов. Формат подразумевает

хорошую техническую оснащенность всеми необходимыми инструментами сбора данных.

Межфункциональный центр – на базе возможностей базовой диспетчерской этот формат ЦУПа объединяет и синхронизирует различные функции управления производством: планирование, операционное управление процессами, обеспечение безопасности персонала.

Интеллектуальный или *аналитический ЦУП* – отличается применением ИИ-алгоритмов и моделей для оптимизации работы предприятия через анализ данных, собираемых в режиме реального времени. Например, проекты типа «цифровой рабочий», позволяющие фиксировать деятельность специалистов на объекте датчиками и камерами для мгновенной обработки собираемых данных и автоматической выдачи рекомендаций.

Данные учетных приборов и автоматизированных датчиков собраны на платформе в единую цифровую модель, которая проводит мониторинг и корректировку порядка эксплуатации приборов, разрабатывает мероприятия для устранения неисправностей.

Центр управления цепочками поставок – выполняет задачи поиска оптимального алгоритма взаимодействия между множеством производственных и логистических площадок, включая партнерские и клиентские, на основе анализа данных для максимальной оптимизации производства и сбыта.

Эти модели не взаимоисключающие, они могут дополнять друг друга. Но важно понимать, что без достаточного уровня автоматизации рабочих процессов у сотрудников ЦУПа будет хватать времени только на первичный сбор информации. Тогда как наиболее интересная функция ЦУПа – обработка данных и аналитические задачи.

Для цифровой трансформации производства важно сформулировать комплексные решения, охватывающие все звенья автоматизации предприятия (контрольно-измерительные приборы и средства автоматики, средства измерения, АСУ ТП, MES).

В условиях растущей глобализации экономики производственные предприятия все больше фокусируются на преимуществах ИТ-решений, чтобы в условиях жесткой конкуренции повысить маржинальность бизнес-моделей. ЦУПы на базе передовых цифровых инструментов, например, системы управления производством MES – Manufacturing Execution Systems – становятся базовым элементом стратегии трансформации производства. Это цифровые решения, используемые для документирования, контроля и управления всеми процессами в промышленности в режиме реального времени.

ЦУПы улучшают наглядность и прозрачность операционной составляющей предприятия.

Еще один важный фактор ЦУПа – возможность сращивать управление данными производства в реальном времени с различными платформами, такими как распределенные системы управления (DCS) или системы планирования производства (ERP).

В настоящее время ЦУПы на базе MES наиболее востребованы в проектах нефтегазовых компаний по разработке сложных и удаленных месторождений, объемы которых растут в условиях истощения легкоизвлекаемых запасов. К таким проектам предъявляются более высокие требования в плане эффективности и оптимизации процессов, сокращения влияния человеческого фактора.

ЦУПы и развитие промышленной автоматизации благодаря MES-инструментам помогают добывающим компаниям преодолевать типичные отраслевые вызовы: разрозненность данных диспетчерских служб и их устаревание, сложности фиксации добытого сырья от уровня партии в трубе до ж/д-цистерны или даже бочки. Переход от простой автоматизации технологических процессов к цифровизации и далее к ЦУП отражен на рис. 2.2.

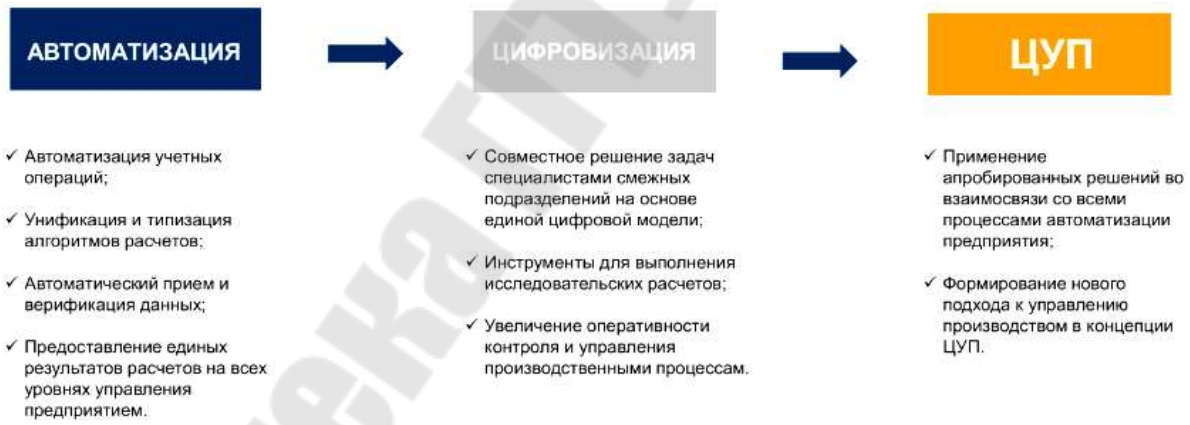

Рис. 2.2. Переработка и производство

На рис. 2.3 представлена схема интегрального дистанционного мониторинга фактического состояния технологических установок, которая показывает движение информации о параметрах работы технологических установок – от полевых устройств до центра удаленного мониторинга и диагностики технического состояния оборудования.

Рис. 2.3. Интегральный дистанционный мониторинг фактического состояния технологических установок

В общем случае MES-система представляет собой комплекс программных и аппаратных средств для координации процессов на производстве и позволяет:

– отслеживать распределение ресурсов;

– контролировать производство на основе информации из других систем;

– визуализировать информацию о месте и времени изготовления продукции;

– сравнивать плановые и фактические показатели производства и т. п.

MES-системы не управляют физическим оборудованием. Они собирают данные из PLC (системы программируемых логистических контроллеров) и SCADA (системы управления и сбора данных). Те, в свою очередь, взаимодействуют с оборудованием или получают информацию с датчиков через IoT-платформы.

На основе этих данных MES управляет производственными заданиями и отправляет результаты анализа персоналу. Интеграция MES поможет автоматически собирать данные из производственных систем без участия человека и эффективнее контролировать процессы на предприятии.

Программное обеспечение MES охватывает службы персонала, обслуживание буровых станков, качалок для добычи нефти и вспомогательных подразделений производственного предприятия, процессы

закупок и отгрузки, контроля запасов, технического обслуживания и планирования деятельности. Преимущества предприятия с системой MES изложены в табл. 2.1.

Таблица 2.1

Сравнение двух типов предприятий с системой управления производством MES и без нее

Предприятие без MES	Предприятие с MES
Не связанные между собой системы	Единая платформа для управления производственными процессами
Ручная передача информации между системами	Автоматический обмен информацией в реальном времени
Возможны задержки в работе предприятия	Быстрая работа с минимумом простоев
Сложно отследить изменения	Полный контроль над процессами
Высокий риск ошибок из-за человеческого фактора	Человеческий фактор сведен к нулю
Трудности с масштабированием при увеличении объемов производства	Легкая адаптация к росту бизнеса

Чтобы MES-система работала, нужно соединить датчики, сенсоры и RFID-метки с софтом. Современные MES-системы разрабатывают при помощи технологии IoT. Так обмен информацией происходит автоматически через Интернет (https://www.purrweb.com/).

Платформа работает на принципах технологии промышленного Интернета вещей, суть которой – объединение информации, переданной со всех датчиков с системами, алгоритмами мониторинга данных, большими данными и приложениями. В системе должна быть реализована ролевая модель. Визуальный контроль и оперативный анализ технологических процессов скважин реализуется на мнемосхемах в табличном виде и в форме трендов. Применяется визуальный контроль цветовой сигнализации выхода измеряемых параметров объектов за допустимые границы, а также состояний на объектах.

Можно выделить следующие рабочие процессы для построения MES-системы в нефтедобыче:

– контроль и оперативный анализ работы скважин (фонтанных, ШГН, УЭЦН);

– контроль и оперативный анализ работы технологических процессов, связанный с автоматизированной системой измерений массы сырой нефти, массы сырой нефти без учета воды (обезвоженной неф-

ти) и объема свободного нефтяного газа, за определенный период времени (АГЗУ);

– контроль и оперативный анализ работы вспомогательных объектов (булиты, маслозаправочные установки (МЗУ), дозаторы и др.);

– контроль и оперативный анализ работы нагнетательных скважин и объектов цехов по поддержке пластового давления (далее – ЦППД);

– контроль и оперативный анализ работы площадных объектов (резервуары, узлы учета).

Еще одна система, которая окажет значительное влияние на финансовые показатели, – контроль и оперативный анализ работы объектов энергоснабжения. Визуальный контроль и анализ работы объектов энергоснабжения и потребления электроэнергии на основании данных, получаемых из систем АСКУЭ и СТАУЭЭ либо из систем их замещающих, включая энергоконтроль, направленный на регулирование «пиковых нагрузок».

Платформа работает на открытой микросервисной архитектуре, ее использование позволяет значительно ускорить процесс разработки и внедрения ИТ-приложений для эффективного управления непрерывным производственным процессом.

Внедрение ЦУП на основе MES-системы для автоматизации производственных процессов способствует следующим эффектам:

– создает инновационную микросервисную архитектуру с внедрением современных технологий для управления и контроля за непрерывным производством;

– формирует общую систему верификации структурированных данных для всех систем управления производственными процессами;

– обеспечивает легкий доступ к данным, в том числе для формирования управленческой отчетности;

– обеспечивает сокращение сроков внедрения цифровых систем за счет быстрого доступа к данным;

– влияет на скорость взаимодействия с источниками данных и системами управления технологическими процессами;

– интегрирует сторонние решения на базе платформы с возможностью размещать бизнес-приложения в периметре платформы.

MES-системы на данный момент стали основным инструментом управления производственными процессами с уровня единой цифровой диспетчерской. MES-инструменты связывают администрацию предприятия и процесс принятия решений с ситуацией на линиях

производства в реальном времени. Именно они делают ЦУПы тем, чем они являются – центрами управления производственными процессами.

Обычно на предприятиях, занимающихся несколькими видами производственной деятельности, внедряется столько MES-систем, сколько существует различных производственных процессов. Если взять классический пример вертикально-интегрированной нефтяной компании, то для процессов добычи нефти и процессов переработки нефти и процессов отпуска нефтепродуктов на АЗС невозможно использовать единую MES-систему, так как функционал программных продуктов, необходимый для реализации бизнес-процессов каждого направления, весьма уникален. Единым компонентом MES-систем для всех этих процессов может послужить база данных временных рядов, в которую в режиме реального времени поступают данные для обработки и аналитики другими приложениями. В литературе часто такую базу данных называют озером промышленных данных. Стоит отметить, что данные этого так называемого озера могут использоваться не только уровнем MES, но и уровнем ERP.

Поэтому решения для ЦУП являются результатом консолидации реальных кейсов, сформированных на потребностях заказчиков.

2.2. Цифровые экосистемы

Инновационное развитие экономики способствует росту и развитию цифровых экосистем, увеличению количества участников и технологическому совершенствованию предоставляемых сервисов. В стратегические планы входит активное внедрение экосистемной модели и на белорусских предприятиях.

Прежде всего успешность формирования цифровых экосистем будет определяться развитием цифровых технологий. Наиболее востребованными и быстро развивающими в 2022–2025 гг. стали облачные вычисления, Интернет вещей, RFID-технологии и технологии ИИ, промышленные роботы, цифровые двойники и аддитивные технологии. Каждая из технологий оказала влияние на становление рынка цифровых экосистем (рис. 2.4).

Рис. 2.4. Становление рынка цифровых экосистем

Концепция цифровых бизнес-экосистем была выдвинута в 2002 г. группой европейских исследователей, которые применили метафору природной экосистемы к миру информационно-коммуника-ционных технологий. В их понимании цифровая экосистема – это распределенная адаптивная система, которой свойственны такие природные качества, как самоорганизация, масштабируемость и устойчивость.

Сегодня под цифровой экосистемой, как правило, понимают комплекс информационных систем, технологий, ИТ-продуктов и сервисов, взаимодействующих между собой и образующих единую сеть. Эта концепция выходит за рамки традиционной ИТ- и бизнес-инфраструктуры и включает широкий спектр элементов – от конечных клиентов, облачных вычислений, серверов и анализа данных до приложений на базе ИИ и датчиков Интернета вещей. В сумме они образуют целостную среду, которая способствует инновациям и беспрепятственному взаимодействию пользователей. Появление экосистем – естественный шаг в развитии современных цифровых продуктов, потому что они предлагают наиболее полный, удобный и интегрированный опыт для пользователей.

Цифровые экосистемы могут быть интерпретированы как цифровые аналоги биосистем. Термин новый, неоднозначный и в практи-

ке его использования существуют разночтения в его толковании [2]. В цифровой повестке Евразийского экономического союза [3] цифровые экосистемы рассматриваются как открытые и устойчивые системы, которые включают в себя физические, юридические, виртуальные субъекты, а также их связи и отношения в цифровой форме. В соответствии с действующим белорусским законодательством экосистема цифровой экономики – это открытая устойчивая информационная среда, обеспечивающая постоянное взаимодействие цифровых платформ, функционирующих на них сервисов, информационных систем.

Цифровую экосистему можно определить как совокупность платформ различного функционала и чаще всего с общим интерфейсом, обеспечивающую применение клиентоцентричной бизнес-модели и объединяющую значимое число участников в рамках бесшовного интегрированного процесса в качестве отдельного этапа ее жизненного цикла.

В целом цифровая экосистема – это комплекс внутренних систем и приложений, бизнес-процессов, поставщиков, партнеров и клиентов (рис. 2.5).

Рис. 2.5. Обобщающая схема цифровой экосистемы

Ключевые компоненты современной цифровой экосистемы:

– *инфраструктура*: облачные и внутрикорпоративные платформы, лежащие в основе цифровых экосистем, обеспечивают масштабируемость, гибкость и доступность цифровых услуг;

– *аналитика данных*: использование больших данных и инструментов аналитики помогает получить ценные инсайты для принятия взвешенных управленческих решений;

– *интеграционные платформы*: бесшовная интеграция различных приложений и систем формирует единую и эффективную цифровую среду;

– *протоколы безопасности*: надежные меры кибербезопасности защищают конфиденциальные данные и обеспечивают целостность цифровой экосистемы;

– *инструменты для совместной работы*: платформы, которые облегчают сотрудничество, коммуникацию и обмен знаниями между сотрудниками в режиме реального времени.

Цифровые экосистемы также подразделяются на открытые, закрытые и гибридные.

Открытые экосистемы состоят из общераспространенных продуктов с открытой лицензией и продуктов с бесплатным кодом (оплачивается только их поддержка). Оператор не ограничивает внутреннюю конкуренцию поставщиков продуктов и публикует недискриминационные критерии присоединения участников.

Закрытые системы – это замкнутые в себе сети ИТ-решений; софт, который работает только с определенными шинами передачи данных и поддерживает определенные стандарты обмена данными, действующие только в рамках этих решений. Интеграция подобных систем с «внешним миром» затруднительна или невозможна. Классический пример закрытой экосистемы – iOS.

Ранее в целях безопасности крупные нефтегазовые корпорации старались строить именно супернадежные закрытые экосистемы с независимыми каналами коммуникаций и ключом шифрования данных.

На сегодняшний день самый распространенный вариант – *гибридная модель*, сочетающая в себе открытые и закрытые платформенные решения (https://trends.rbc.ru/trends/industry/65cc6eff9a79477bbf222ed0?from=copy).

Создание успешной цифровой экосистемы требует тщательного планирования. Разработчики должны учитывать такие факторы, как:

– *масштабируемость*: строить с учетом будущего роста, гарантируя, что экосистема сможет адаптироваться к меняющимся потребностям бизнеса;

– *функциональная совместимость*: обеспечить плавную интеграцию новых технологий и устаревших систем, чтобы избежать разрывов и несостыковок данных;

– *кибербезопасность*: отдавать приоритет надежным мерам безопасности для защиты от киберугроз и обеспечения конфиденциальности информации;

– *пользовательский опыт*: проектировать с учетом потребностей конечного потребителя, создавая интуитивно понятные интерфейсы и оптимизируя все процессы;

– *гибкость*: развивать культуру гибкости и адаптируемости для реагирования на изменения рынка и технологические инновации;

– *наследуемость*: необходимо с самого начала вести учет и описание процессов автоматизации, создавать инструмент передачи и масштабирования знаний по ней среди специалистов и потребителей.

2.3. Цифровизация и автоматизация добычи газа и нефти

Основой оптимизации процессов добычи нефти и газа при применении цифровых технологий является интеграцией отдельных апробированных на объектах решений в единый интегрированный технологический комплекс, обеспечивающий динамическую оптимизацию и повышение качества управления на базе реальных параметров и геолого-геофизической информации по всей технологической цепочке добычи – от цифровых скважин до подготовки продукта к транспорту, непрерывного анализа эффективности управляющих воздействий и моделирования технологических особенностей месторождения в реальном времени.

Усовершенствование автоматизации добычи газа представляет собой применение передовых информационных технологий, сенсорных систем, аналитики данных и ИИ для оптимизации процессов добычи. Современные цифровые технологии позволяют снизить риски и затраты, повысить производительность и безопасность работников, минимизировать выбросы углеводорода в окружающую среду. Повышенная сложность выполнения этих работ требует установку и использование современного цифрового оборудования для добычи, транспортировки и обработки газа.

В газодобыче существуют различные технологии и инструменты автоматизации, которые помогают улучшить эффективность и безопасность процесса добычи газа. Обычно они включают в себя:

– *системы удаленного мониторинга и управления добычей газа*, которые позволяют оператору дистанционно контролировать ключе-

вые параметры технологического оборудования, производить ее запуск/остановку в строгом соответствии с установленным регламентом и выполнять другие функции, поддерживаемые компьютерным оборудованием автоматизированных систем управления;

– *автоматические системы управления*, которые без участия оператора обеспечивают контроль и оптимизацию параметров работы скважин, таких как давление и расход газа. Сегодня для этого применяются различные алгоритмы: позиционные, пропорционально-интегрально-дифференциальные (ПИД), усовершенствованные (APC), модельные с предсказанием (MPC, fuzzy, нейросетевые), киберфизические, использующие модели цифровых двойников. Все они облегчают работу оператора и за счет высокой скорости обработки событий обеспечивают приемлемую аварийную защиту и оперативное выполнение действий по поддержанию оптимальных условий добычи;

– *роботизированное обслуживание скважин*. Такие системы выполняют сложные мехатронные операции по обслуживанию скважин без участия человека. Они могут проводить ремонтные работы, заменять оборудование и осуществлять технологические операции с высокой точностью и безопасностью;

– *системы компьютерного мониторинга в реальном времени по месту расположения скважин на месторождении газа*. Эти системы позволяют операторам получать информацию о работе скважин в режиме реального времени. Они оснащены оптическими и акустическими датчиками, которые могут мониторить состояние оборудования и определять возможные проблемы на ранних стадиях их развития.

Умная автоматизация добычи газа может быть реализована в РФ с применением следующих средств:

1. Система подачи ингибитора «СПИ-02». Эта система обеспечит подачу ингибитора в трубопровод для предотвращения образования либо для разрушения образовавшихся гидратов.

2. Двухфазный расходомер газа «ДФР-01». Это новое изделие, в котором реализовано решение по измерению двухфазного потока добычи газа методом переменного перепада давления на двух сертифицированных средствах измерениях – расходомере газа «Гипер-Флоу» и диафрагменном узле оригинальной конструкции.

3. Регулирующее устройство дебита газовой скважины «РУД-02» обеспечит регулирование дебита в широком динамическом диапазоне.

4. Диспетчерский комплект обеспечит прием, архивирование,

отображение полученной информации, а также передачу команд в блок электроники кустового комплекта [5].

Эти программно-аппаратные средства позволяют реализовать усовершенствованную (умную) автоматизацию процесса добычи газа на основе программно-аппаратных средств, показанных на функциональной схеме IOT сбора информации и предоставления ее для принятия управленческих решений оператору (рис. 2.6).

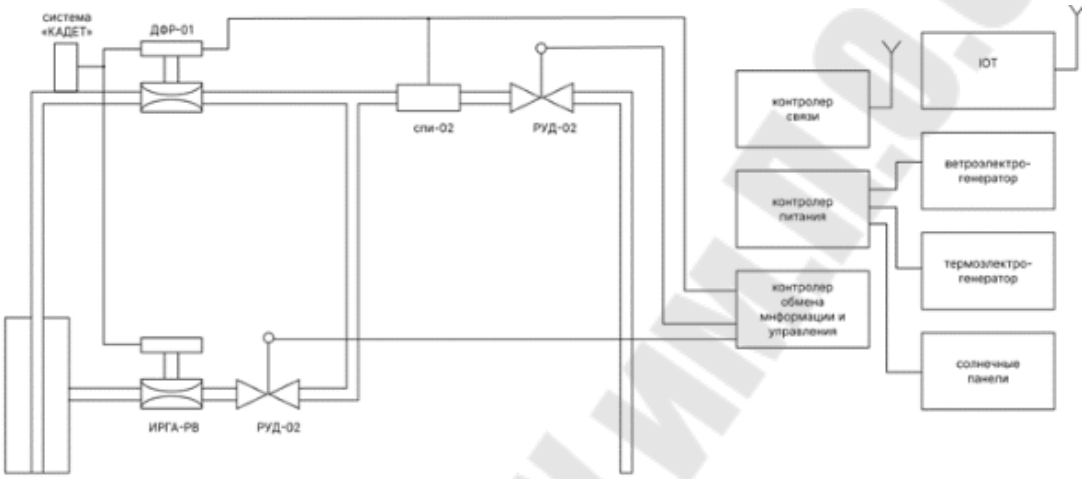

Рис. 2.6. Функциональная схема добычи газа

На объектах устанавливаются датчики технологических процессов и исполнительные механизмы, коммутируемые с устройствами сопряжения, которые образуют «нижний уровень» беспроводной системы контроля и управления. Структурная схема беспроводного управления приведена на рис. 2.7. Электропитание устройств «нижнего уровня» (измерительные приборы, исполнительные механизмы и т. п.) (рис. 2.8) может быть как энергозависимым (внешние электрические сети), так и полностью энергонезависимым, т. е. локальным (солнечные батареи, аккумуляторы).

Комплекс реализован на базе модулей автоматизированной системы объектовой информации АСОИ «Скважина» для территориально распределенных объектов, не имеющих линий связи и электроснабжения на оборудовании беспроводных сенсорных сетей (БСС) (рис. 2.8).

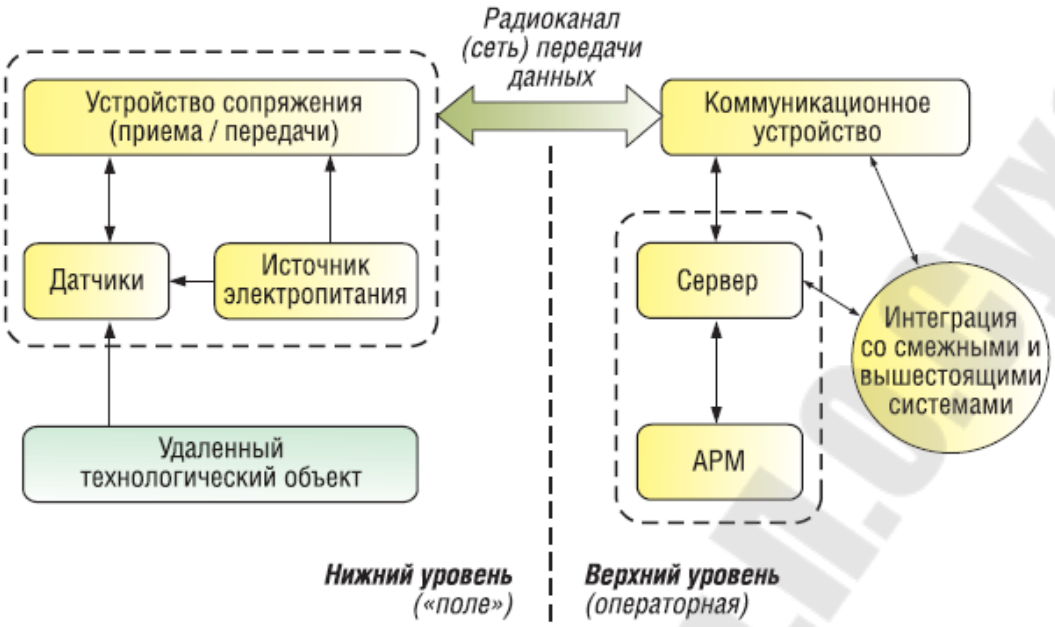

Рис. 2.7. Структурная схема беспроводного управления объектами

Рис. 2.8. Общая схема беспроводной передачи данных

В состав АСОИ «Скважина» входит проектно-компонуемый набор устройств измерения технологических параметров объекта и энергонезависимых беспроводных каналов связи. Каждая из 90 имеющихся эксплуатационных скважин рассматривалась как самостоятельный объект автоматизации с оборудованием: четыре измерительных сенсорных модуля давления (СМД), измеряющих буферное, межколонное, затрубное давление и давление газа на выходе скважины; по одному сенсорному модулю температуры (СМТ), измеряющему температуру газа на выходе скважины и модулей связи (маршрутизаторы) МСиС.

Модули для измерения давления и температуры устанавливаются на штатные места фонтанной арматуры, предусмотренные для местных манометров и термометров, поэтому установка датчиков и их демонтаж не требуют выполнения сложных монтажных и сварочных работ. Определение дебита скважины проводится на основании измерений буферного и затрубного давлений. Организация системы телеметрии АСОИ «Скважина» представлена на рис. 2.9.

Рис. 2.9. Датчики и маршрутизаторы на арматуре скважины

Данные от сенсорных модулей давления и температуры скважин поступают на сервер и выводятся на АРМ геолога в виде мнемосхем, таблиц и графиков (трендов). Геолог на основе заданного режима ра-

боты ПХГ (закачка, отбор) и имеющихся методик определяет требуемые для эффективной работы значения дебита по каждой скважине и выдает их в качестве задания диспетчеру ПХГ или оператору. Наличие оперативной и объективной информации о функционировании каждой скважины позволяет геологу или технологу делать выводы об эффективности работы скважин и планировать мероприятия по их реконструкции, капитальному ремонту и ликвидации.

Диспетчер (технолог) изменяет дебиты скважин в соответствии с полученным заданием путем управления регулирующей арматурой, установленной на газосборном пункте (ГСП) через АРМ АСУ ТП, и контролирует изменение дебита на АРМ диспетчера. Накопленные результаты мониторинга дают возможность обеспечить контроль последовательности действий персонала по управлению контрольными и управляющими узлами на линии «скважина – газосборный пункт» для любого интервала времени, включая и случаи возможного возникновения нештатных ситуаций, что обеспечивает важность для безопасности эксплуатации подземного хранилища газа и месторождений. Установка датчиков и маршрутизаторов БСС приведена на рис. 2.10.

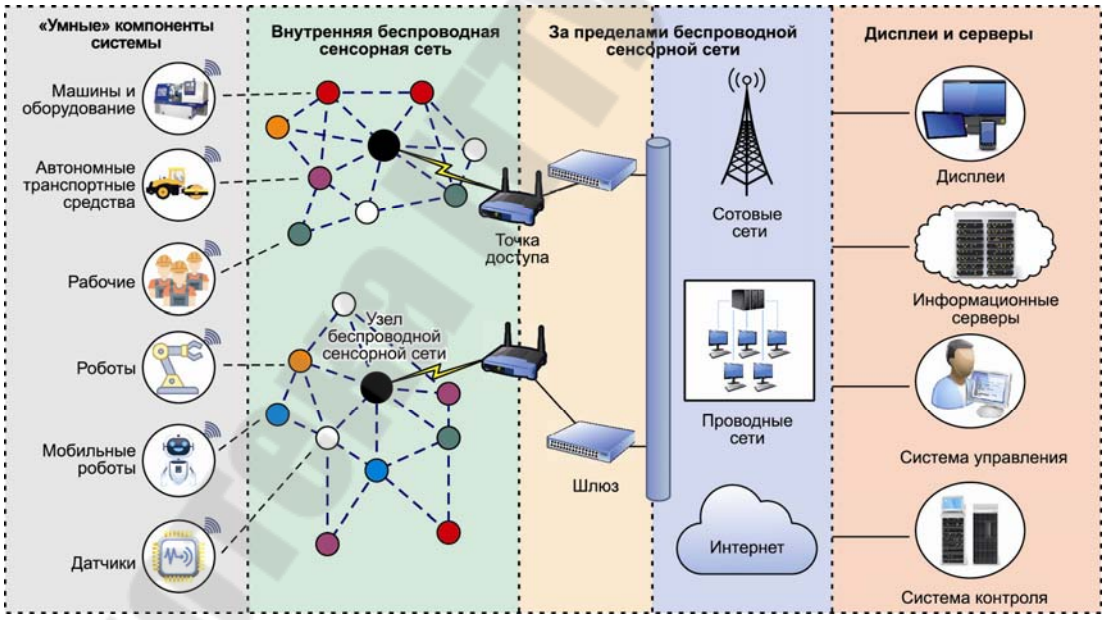

Рис. 2.10. Установка датчиков и маршрутизаторов беспроводных сенсорных сетей

Одним из важнейших технологических параметров работы скважины является своевременное обнаружение в газовом потоке твердых фракций (песка), выносимых из скважины. Регистрация сигнала, вызванного соударением песчинок, позволяет в режиме реаль-

ного времени получать непрерывный тренд изменения концентрации песка в газе.

Особенностью сенсорных сетей является способность системы к динамической самостоятельной организации сети передачи данных, в отличие от большинства беспроводных измерительных приборов, которые требуют наличия прямой видимости между прибором и центральной приемной станцией. Применяемые решения обеспечивают возможность полевому оборудованию взаимодействовать между элементами системы.

Связь между модулями системы осуществляется на разрешенных частотах для систем контроля и не требует получения специальных разрешений. Компоненты системы позволяют создавать энергонезависимые сети сбора информации до тысяч точек контроля при их территориальном распределении на площади до 100 км^2 и обеспечении расстояния между этими точками до 2 км. С применением выносных узконаправленных антенн дальность передачи данных увеличивается до 15 км. Количество и набор установленных измерительных датчиков определяется для каждой скважины индивидуально.

Подобные системы (рис. 2.11) сегодня нашли широкое применение при реконструкции месторождений.

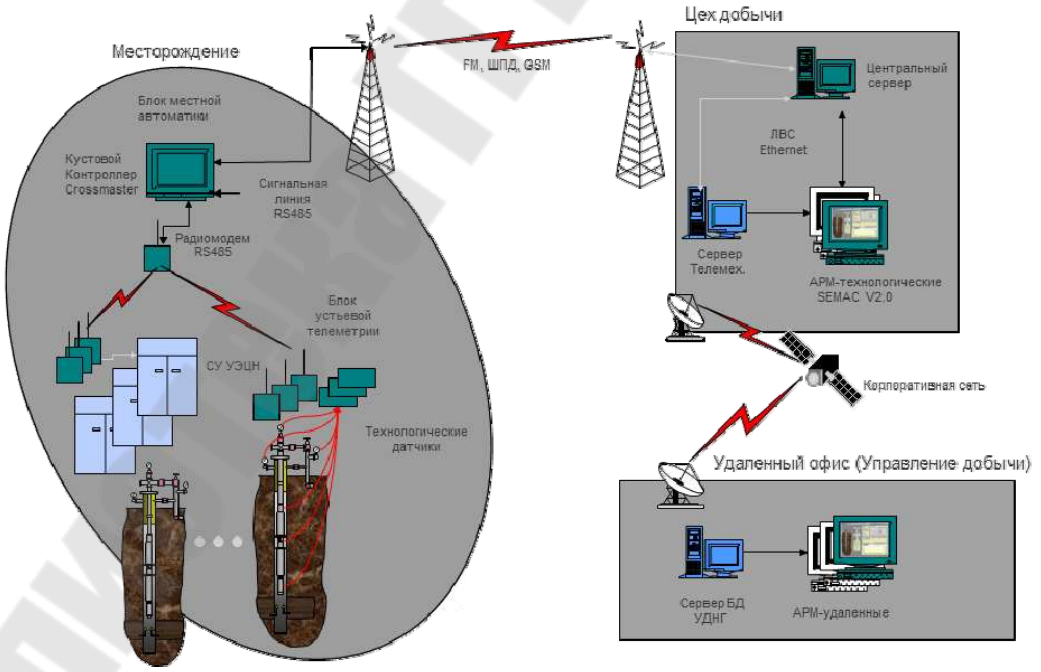

Рис. 2.11. Схема передачи сигналов от технологических датчиков в скважине через блок устьевой телеметрии на месторождении в цех добычи и управления добычи

Данные системы предназначены:

– для обеспечения контроля и мониторинга технологических параметров объектов (скважин) в условиях отсутствия постоянного энергоснабжения (имеются датчики давления, перепада давления, температуры, уровня, дискретные, сигнализаторы, наличия твердых примесей, виброконтроля, влажности и других параметров);

– периодического измерения параметров эксплуатационных скважин в точках измерений и заданного временного интервала, оперативной передачи данных по каналам наземной радиосвязи или спутниковой связи на центральный пункт;

– надежного функционирования системы в условиях естественного уровня радиопомех и пиковых нагрузок в сотовых сетях;

– автоматического использования канала гарантированной доставки в случае отсутствия или нарушений в каналах оперативной связи;

– сбора, систематизации и анализа получаемой информации, визуализации на местах;

– обеспечения взаимодействия «человек – машина» с использованием АРМ специалиста геологической службы СПХГ, ДКС, ГСС, кустов скважин и других объектов;

– формирования отчетов о значениях параметров эксплуатационных скважин;

– накопления информации о режимах работы скважин для анализа и эксплуатации.

2.4. Использование цифрового двойника в нефтегазовой отрасли

Цифровой двойник (digital twin) представляет собой виртуальную модель физического объекта или системы, обновляемую в реальном времени на основе данных с сенсоров и других источников.

В нефтегазовой отрасли цифровые двойники используются для повышения эффективности, безопасности и устойчивости процессов на всех этапах производства, включая разведку, добычу, транспортировку, переработку и распределение.

Современная нефтегазовая промышленность сталкивается с рядом проблем, включая высокую степень технической сложности, необходимость соблюдения строгих стандартов безопасности и экологических норм, а также потребность снижения затрат и повышения операционной эффективности. Технология цифровых двойников пре-

доставляет уникальные возможности для решения этих задач, позволяя создавать точные виртуальные модели реальных объектов и процессов, которые могут использоваться для анализа, оптимизации и прогнозирования работы производственных систем.

Применение цифровых двойников в нефтегазовой отрасли

1. Разведка и добыча

Цифровые двойники играют важную роль в разведке и добыче нефти и газа, обеспечивая создание высокоточных моделей месторождений и скважин (рис. 2.12).

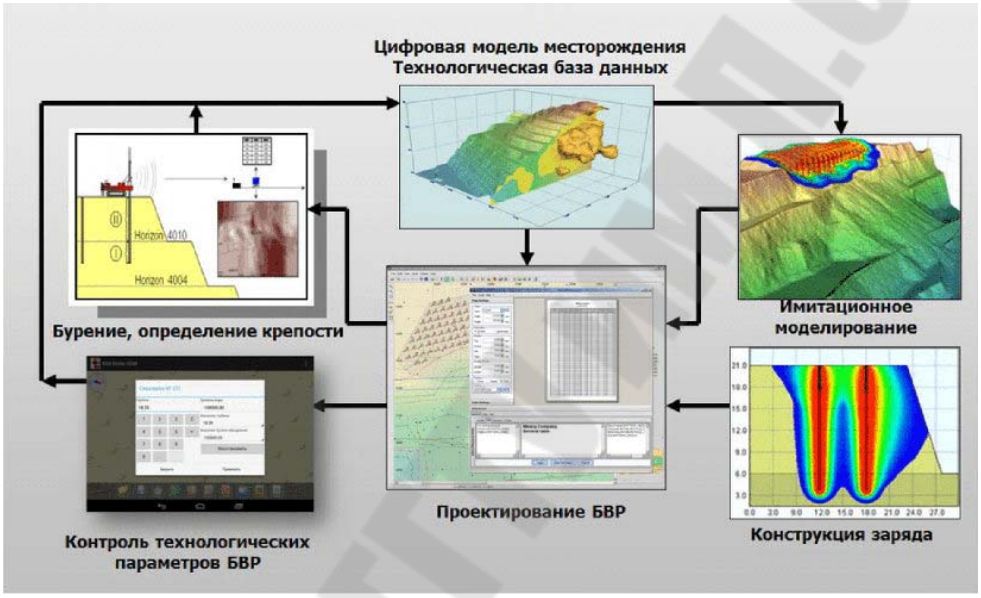

Рис. 2.12. Схема построения модели месторождения

Эти модели позволяют:

– *улучшить точность прогнозирования запасов*: использование данных с датчиков и геофизических исследований для создания детализированных моделей месторождений;

– *оптимизировать бурение*: моделирование буровых операций с учетом текущих данных о состоянии скважины и геологических условиях, что снижает риски и повышает эффективность бурения;

– *мониторинг состояния скважин*: реализация системы мониторинга с использованием цифровых двойников для отслеживания параметров работы скважин и своевременного выявления и устранения аномалий.

2. Транспортировка и хранение

В области транспортировки и хранения нефти и газа цифровые двойники используются для следующих процессов:

– *мониторинга состояния трубопроводов и резервуаров*: постоянный сбор и анализ данных с датчиков для выявления утечек, коррозии и других потенциальных проблем. Мониторинг технического состояния может осуществляться с помощью волоконно-оптической системы мониторинга (рис. 2.13) и системы дистанционного коррозионного мониторинга;

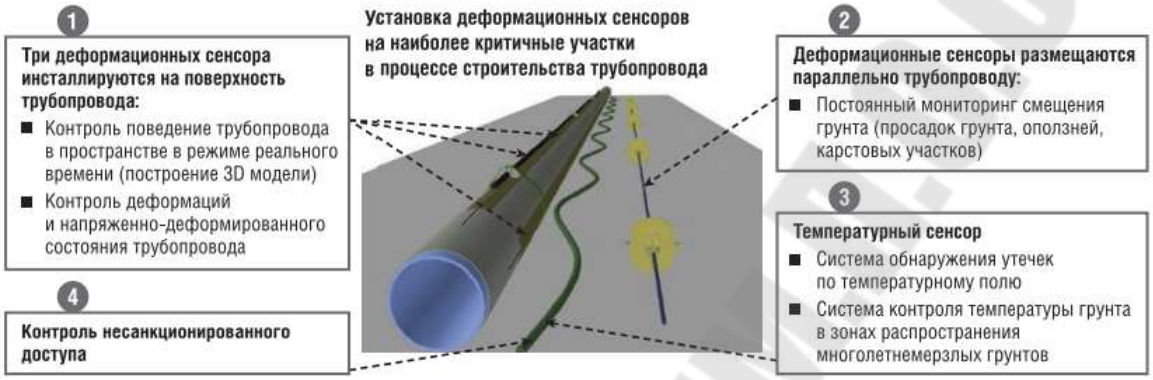

Рис. 2.13. Волоконно-оптическая система мониторинга (https://magazine.neftegaz.ru/articles/transportirovka/549187-podlednyy-maintenance-tekhnologii-monitoringa-tekhnicheskogo-sostoyaniya-obsluzhivaniya-i-remonta-po/)

– *оптимизации эксплуатации трубопроводных систем*: моделирование работы трубопроводов и резервуаров для повышения их надежности и эффективности, а также минимизации рисков аварийных ситуаций.

3. Переработка и производство

В переработке и производстве нефтехимических продуктов цифровые двойники помогают:

– *оптимизировать технологические процессы*: моделирование производственных процессов для повышения их эффективности, снижения энергопотребления и улучшения качества продукции;

– *предсказывать и предотвращать неисправности*: использование предиктивной аналитики для прогнозирования и устранения возможных сбоев в работе оборудования.

4. Управление цепочками поставок

Цифровые двойники способствуют улучшению управления цепочками поставок, обеспечивая:

• Реалистичное моделирование логистических процессов: оптимизация маршрутов доставки, управление запасами и улучшение планирования поставок (рис. 2.14).

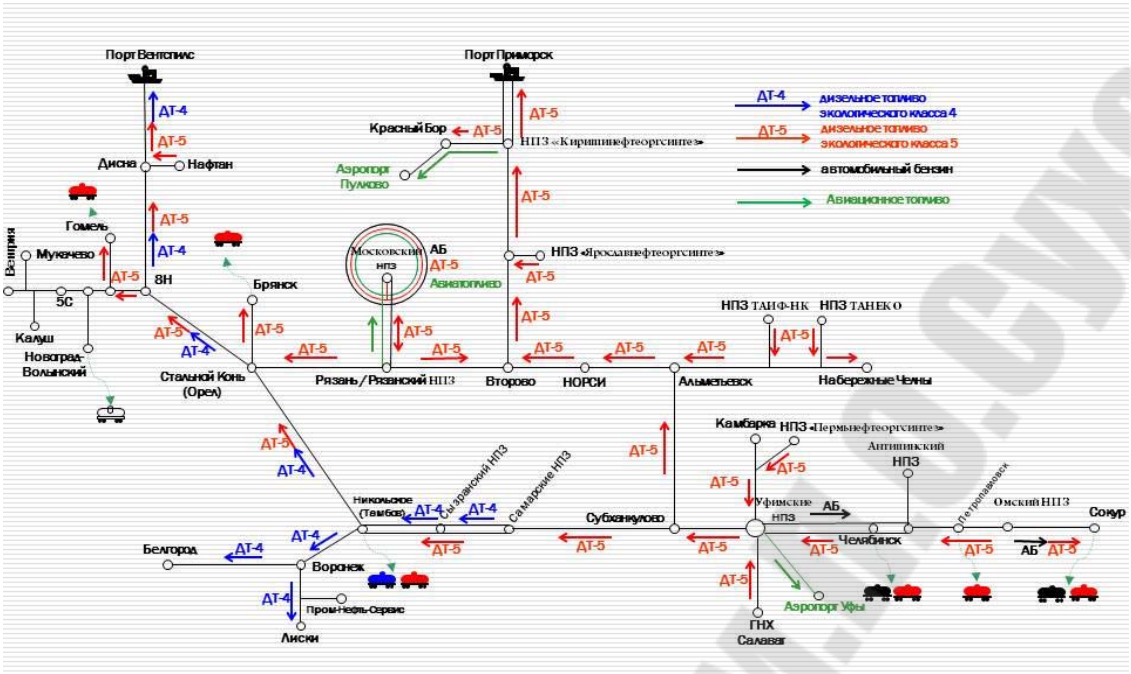

Рис. 2.14. Пример схемы моделирования логистических процессов грузопотоков нефтепродуктов

• Повышение прозрачности и оперативности принятия решений: анализ и синхронизация данных по всей цепочке поставок для сокращения времени отклика на изменения в рыночной конъюнктуре и оперативного реагирования на чрезвычайные ситуации.

Преимущества использования цифровых двойников:

– *повышение эффективности*: позволяют оптимизировать процессы, снизить издержки и увеличить производительность;

– *улучшение безопасности*: реальный мониторинг состояния оборудования и процессов помогает своевременно выявлять и устранять риски, что снижает вероятность аварий.

• Устойчивое развитие: снижение экологического воздействия и повышение энергоэффективности производства благодаря оптимизации технологических процессов.

Вызовы и перспективы развития:

1. *Интеграция данных и кибербезопасность.* Одним из главных вызовов является интеграция данных с различных источников и обеспечение их безопасности. Разработка эффективных систем управления данными и внедрение современных методов защиты информации являются критически важными задачами.

2. *Квалификация персонала и обучение*. Для эффективного использования цифровых двойников необходимы высококвалифицированные специалисты, способные разрабатывать, внедрять и поддер-

живать эти системы. Обучение и повышение квалификации работников отрасли становятся неотъемлемой частью процесса цифровой трансформации.

3. *Инновации и технологическое развитие*. Будущее цифровых двойников связано с развитием технологий ИИ, машинного обучения и больших данных. Прогнозируется дальнейшее совершенствование алгоритмов анализа и моделирования, что позволит значительно расширить возможности цифровых двойников и улучшить их интеграцию с другими системами.

Таким образом, внедрение цифровых двойников является важным шагом на пути к созданию более современной, эффективной и безопасной нефтегазовой промышленности. Ожидается, что с развитием технологий и совершенствованием методик, цифровые двойники будут играть все более значимую роль в трансформации отрасли, способствуя достижению стратегических целей и устойчивому развитию энергетического сектора.

2.5. Интеллектуальное (цифровое) месторождение: понятие и структура

Создание цифровых двойников месторождения (ЦДМ) входит в топ-5 востребованных трендов в нефтегазовой отрасли. Цифровой двойник месторождения является виртуальным отображением происходящих процессов в режиме реального времени, что позволяет оперативно реагировать и корректировать работу добывающих скважин, оборудования и персонала [10].

Необходимо отличать ЦДМ от цифрового двойника актива (ЦДА). Цифровой двойник месторождения есть отражение системы «пласт – скважина – сеть сбора», т. е. производственная модель, так как работа ЦДМ направлена на решение вопросов, связанных с добычей углеводородов.

Цифровой двойник месторождения является составной частью ЦДА, так как появляются дополнительные звенья, такие как энергетика, кадровый состав и другие участки основного и вспомогательного производства. Цифровой двойник актива является бизнес-моделью, так как основные целевые ориентиры определяются экономическими критериями, в частности такими, как объемы получаемой прибыли, показатели экономической эффективности геолого-технических мероприятий (ГТМ) и других инвестиционных проектов в разработке месторождений.

Эволюция промысловых цифровых технологий происходила от простого к сложному: от измерений, учета, анализа и агрегирования промысловых данных до аналитических систем, решающих задачи в масштабе месторождений, объединенных единой сетью сбора.

С начала XX в. и по настоящее время главным фактором обеспечения прорыва с точки зрения поиска оптимальных решений в области разработки и эксплуатации месторождений становится ускорение обработки данных и устойчивое обоснование решений путем применения интеллектуальных технологий [2].

Такие компьютерные информационные системы позволяют обеспечить автоматизацию сбора, фильтрации, хранения и обработки данных, описать физические процессы, прогнозировать добычу углеводородов и визуализировать ключевые параметры для управленческих решений. Основными задачами при создании таких систем являются контроль большого массива нефтепромысловой информации, качественная ее обработка и отображение в доступной для восприятия форме. В период с 2000-х гг. ведущие нефтегазовые компании и их научно-исследовательские центры начали разрабатывать широкий спектр новых методов информационного управления месторождениями [3]. Технология нового поколения, основанная на внедрении комплекса аппаратных, технических и программных средств в производственные процессы нефтегазодобывающих предприятий, получила различные названия и конфигурацию элементов, входящих в ее систему (рис. 2.15).

Рис. 2.15. Компоненты интеллектуального месторождения и их функции

Каждая компания дает собственное определение технологии исходя из понимания необходимых в данный момент методов решения производственных задач. В литературных источниках приводится множество определений, в их числе:

– интеллектуальное месторождение – это динамическая система взаимосвязанных технологий и бизнес-процессов, обеспечивающих повышение экономической эффективности всех элементов производства и управления нефтегазовым активом [4, 5];

– цифровое месторождение – это программное обеспечение, включающее набор приложений, которые позволяют описывать поведение месторождения на компьютере [6];

– интеллектуальное месторождение – это формирование дополнительной ценности нефтегазового актива путем создания цикла сбора данных, моделирования, принятия решений и их исполнения [7];

– интеллектуальное нефтегазовое месторождение – это система оперативного управления нефтегазовым промыслом, включающая набор бизнес-процессов, направленных на оптимизацию добычи и сокращение финансовых потерь путем своевременного выявления проблем и быстрого принятия решений многопрофильными группами на основе данных, полученных в режиме реального времени, и предусматривающая непрерывную оптимизацию интегральной модели месторождения и управления операциями по добыче нефти (рис. 2.16).

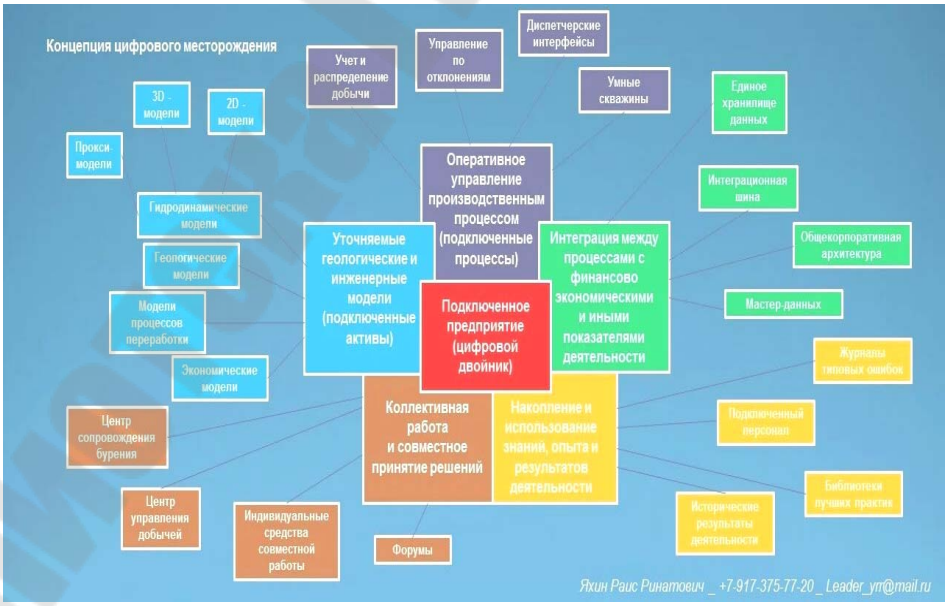

Рис. 2.16. Схема-концепция цифрового (интеллектуального) нефтяного месторождения (https://avatars.mds.yandex.net/i?id=f916b3033ede33cd55b9069badc1ef58_l-4149382-images-thumbs&n=13)

Тем не менее точного определения, отражающего суть технологии, еще не существует, так как его идеальная архитектура должна обеспечить появление искусственных интеллектуальных систем, что пока не представляется возможным. Однако современное развитие информационных технологий и высокотехнологичного оборудования создает условия для кибернетического управления отдельными элементами месторождения.

Эффективность цифрового месторождения как совокупности интеллектуальных систем обусловливается тесной интеграцией в производственные бизнес-процессы интеллектуального оборудования и аналитических информационных продуктов, которые при выявлении отклонений от нормы дают рекомендации по исключению возможного риска. Качество таких решений обеспечивается совмещением оперативных данных по всем системам месторождения с интегрированной моделью актива, дополненной расчетными библиотеками, позволяющими проводить анализ технологической системы и выдавать специалистам предложения по оптимизации и потенциально возможным потерям в будущем (проактивная защита).

2.6. Интегрированная модель месторождения

Технология «цифрового месторождения» связывает воедино все этапы промышленного освоения актива. Ядром технологии является интегрированная модель месторождения (ИММ), в идеальном варианте имеющая алгоритмы получения и обработки данных удаленных систем контроля разработки месторождения. Интегрированная модель месторождения включает математические модели пласта, флюидов, скважин, наземной инфраструктуры месторождения, построенные на основе всех имеющихся данных по месторождению. Интегрированная модель месторождения позволяет интегрировать модели скважин и системы сбора с более крупными моделями пласта и объектов, а также проводить актуализацию модели в режиме реального времени. На основе ИММ можно провести автоматизацию процессов контроля/мониторинга, прогнозирования работы каждой из составляющих систем месторождения с устранением трудоемких выполняемых вручную процессов. Целью построения ИММ является повышение эффективности не только каждой отдельно взятой системы, но и всего актива в целом с учетом взаимовлияния систем.

Интегрированная модель месторождения дает возможность адекватно оценить текущее состояние работы систем, заранее увидеть возможные проблемы и предложить мероприятия по их предотвращению.

Интегрированная модель месторождения неразрывно связана с понятием интегрированного проектирования, которое появилось в 60-е гг. XX в. и предназначалось главным образом для комплексной оптимизации процессов эксплуатации скважин и работы наземных установок, насосного оборудования и других объектов при моделировании разработки нефтяных месторождений [10].

Сегодня оно эффективно дополняется инструментами ИММ – программами, объединяющими все ключевые дисциплины актива (геология, разработка, бурение и заканчивание скважин, нефтедобыча, обустройство, экономика, экология, анализ рисков), для эффективного бизнес-планирования освоения месторождения [11].

Интегрированная модель представляет собой систему взаимосвязанных компонентов и, как правило, включает в себя: модели пласта, скважины, системы сбора и транспорта продукции, системы поддержания пластового давления, завода (установку предварительного сброса воды и установку подготовки и перекачки нефти), экспорта и экономическую модель.

Часто понятие интегрированной модели используют как синоним термина «цифровой двойник», однако между ними есть существенное различие. Интегрированная модель не обновляется в реальном времени и после построения перестает отражать изменения на месторождении, поэтому ее необходимо периодически актуализировать. Это может занимать несколько месяцев и требует участия большой команды инженеров. С цифровым двойником ситуация обстоит иначе: он должен мгновенно реагировать на все происходящие изменения (например, заметить появление новой скважины, подгрузить по ней данные и интегрировать ее в общую систему) – в идеале без вмешательства человека. Привлечение инженеров, когда двойник запущен, происходит в исключительных случаях.

Основное преимущество интегрированных моделей состоит в их способности комплексно анализировать всю цепочку производственных процессов – от пласта до объектов подготовки продукции. Детальный анализ позволяет формировать реалистичные прогнозы профилей добычи углеводородов с учетом физических и технологических ограничений. Кроме того, интегрированные модели помогают

оперативно оценивать и предупреждать возможные неполадки в ходе эксплуатации месторождений, что повышает надежность и эффективность управления разработкой интегрированных моделей.

Инструменты интегрированной модели месторождения

Для того чтобы исключить или свести к минимуму осложнения в работе месторождения, повысить устойчивость проектного решения к параметрам неопределенности, необходимо синхронизировать процессы развития объектов разработки месторождений и их инфраструктуры. Данный подход может быть реализован с использованием ИММ и требует формирования следующих компонентов ИММ цифрового месторождения:

1) алгоритмов сбора, хранения, структурирования, проверки достоверности и фильтрации данных о месторождении, поступающих из различных источников;

2) инструментов моделирования всех элементов интегрированной системы месторождения (ГГДМ, скважины, система сбора, система подготовки, экономика);

3) интеграции методов инженерного анализа данных на основе их обработки в моделях с алгоритмами поддержки принятия решения.

Инструмент моделирования интегрированной системы месторождения – это специализированное программное обеспечение, которое используется специалистами-экспертами в области геологии, бурения, разработки, обустройства и добычи в научно-техническом центре компании. На основе онлайн-данных и специализированного программного обеспечения специалисты создают ИММ и адаптируют ее к истории разработки. Далее обновленные элементы ИММ дополняются библиотеками алгоритмов обработки информации и в режиме реального времени выдают специалистам на нефтепромысле предложения по оптимизации технологического режима работы систем месторождения на основе технико-экономических показателей ограничения.

Инструменты ИММ дают возможность оценивать перспективы развития актива и «возврата инвестиций» в разные моменты времени. Данная функция ИММ становится особенно востребована в условиях высокой волатильности цены на нефть. Таким образом, результатом вложений в построение ИММ в случае ее реализации как ядра цифрового месторождения становится обеспечение прозрачности и скорости принятия решений в ходе процессов добычи нефти.

Для того чтобы ядро ИММ цифрового месторождения заработало, необходимо провести технологическую трансформацию существующих методов работы сотрудников.

Интеграция ключевых показателей эффективности с моделью технико-экономических ограничений режима и аналитическими инструментами ИММ подготовки управленческих решений будет снижать риски финансовых потерь. При такой системе ИММ становится инструментом снижения геолого-технологической неопределенности параметров месторождения, а модель ограничений с ключевыми показателями эффективности работы мотивирует сотрудников к доскональному изучению месторождения и поиску методов увеличения добычи нефти с наименьшими затратами.

Цифровая трансформация подразумевает изменение организационных процессов и бизнес-модели на основе тех возможностей, которые дают новые цифровые технологии. Компоненты двух этих понятий представлены ниже (рис. 2.17).

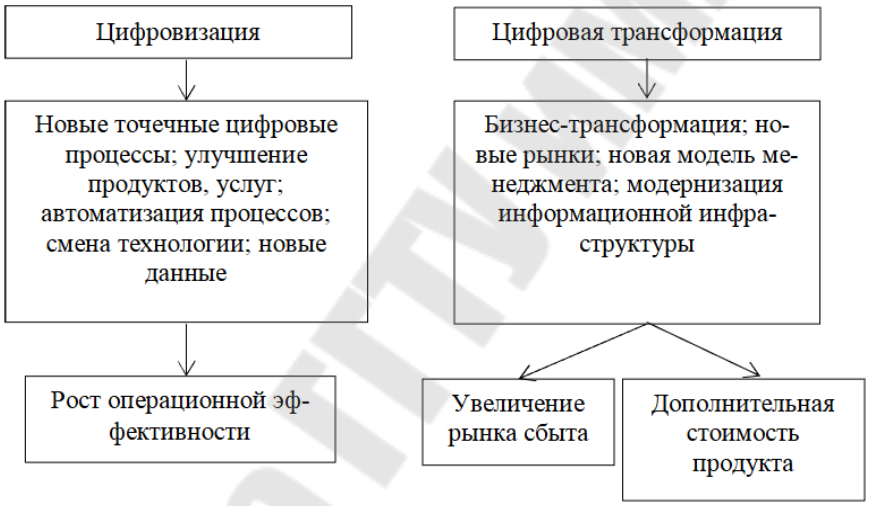

Рис. 2.17. Составляющие «цифровизации» и «цифровой трасформации»

Технология дистанционного (цифрового) управления позволяет обеспечить оперативную динамическую оптимизацию и повышение качества управления процесса добычи за счет алгоритмического формирования управляющих воздействий (рис. 2.18).

В этом процессе изменения качества управления обеспечиваются в реальном времени:

– автоматизированная подстройка и обеспечение адекватности построенной геолого-технологической модели фактическим показателям промысла;

– автоматизированный расчет материального баланса по скважинам и управление режимами кустов скважин, промыслами и месторождению в целом;

– учет ресурсов, планирование работ, оформление отчетных форм с учетом целевых показателей согласно принятой бизнес-модели и ранжирования показателей;

– оптимизация распределения нагрузки по скважинам, агрегатам и установкам, планирование и организация работ по ремонту, обслуживанию и интенсификации;

– адаптация системы управления режимами (СУР) месторождения в реальном масштабе времени, соответствие фактическим показателям моделям рисков и режимов;

– обеспечение технологической и экологической безопасности месторождения.

Рис. 2.18. Структурная схема управления интеллектуальным месторождением

Базовым трендом для цифровых технологий является повторяющийся коррекционный цикл управления:

Измерение → Коррекция → Контроль → Прогноз →
→ Воздействие →Контроль.

При этом важно техническими средствами обеспечить возможность оперативных измерений, для анализа и оперативного регулирования балансов между месторождениями и отборами по кустам скважин и отдельным скважинам. Повышение качества и сроков принятия решений при разработке и эксплуатации газового месторождения обеспечивается за счет:

– получения качественной информации о работе пласта, скважинного и наземного технологического оборудования в реальном масштабе времени;

– диагностирования на базе полученной информации режимами работы скважин и установок, метода капитального ремонта;

– увеличения степени извлечения углеводородного сырья и дебита скважин путем оптимального управления гидродинамическими режимами, оптимальных методов воздействий на пласт.

Основной задачей цифровой трансформации нефтегазовой отрасли является снижение капитальных и эксплуатационных затрат и увеличение эффективности добычи нефти и газа. Цифровая трансформация затрагивает не только производственную деятельность, но и меняет в процессе внедрения организационные структуры, бизнес, а также имеющиеся социальные и образовательные модели.

Назначение АСОДУ

АСОДУ (автоматическая система оперативно-диспетчерского управления) используется для автоматизации и диспетчеризации нефтяных и газовых скважин и других объектов цехового уровня, обеспечивая удаленный контроль параметров и оперативное управление оборудованием через радиоканалы. АСОДУ включает следующие компоненты:

– телеизмерение, мониторинг и регистрация параметров скважин, таких как давление нефти, код ПСМ, счетчик ТОР и др.;

– телесигнализация и регистрация событий, управляющих воздействий и нештатных ситуаций;

– телесигнализация несанкционированного проникновения на удаленный объект (охранная сигнализация);

– обсчет параметров, определение аварий и хранение архива на уровне устройства сбора и передачи данных (УСПД);

– ведение оперативной базы данных параметров;

– визуализация данных на экране автоматизированного рабочего места (АРМ);

– обеспечение доставки информации в диспетчерский пункт;

– возможность расширения системы.

Назначение АСУТП

АСУТП (автоматизированная система управления технологическими процессами) в нефтегазодобывающей отрасли предназначена:

– для автоматизации процессов сбора и получения достоверной информации с технологических объектов;

– оперативного контроля и управления процессами добычи нефти и газа;

– повышения безопасности производства;

– снижения трудоемкости управления технологическими процессами;

– уменьшения простоев оборудования;

– повышения эффективности принятия решений по управлению технологическими процессами на базе единой системы диспетчеризации;

– сокращения численности обслуживающего персонала.

Функции АСУТП НГДО

Основные функции АСУТП в нефтегазодобывающей отрасли включают:

– предоставление качественного удаленного контроля над технологическими процессами;

– обеспечение оперативности действий персонала в штатных режимах и в аварийных ситуациях;

– минимизацию разливов нефти и выбросов газа в аварийных ситуациях за счет быстрого реагирования персонала;

– контроль состояния объектов отрасли;

– автоматизированный оперативный контроль технологических параметров;

– обеспечение точности измерения технологических параметров;

– гарантию надежности работы технологического оборудования;

– обмен данными со смежными информационными системами;

– внедрение современных методов контроля и управления объектами;

– интеграцию различных типов объектов в единую информационную систему;

– организацию доступа к информации на современном уровне;

– обеспечение безопасности информации.

Автоматизация и диспетчеризация нефтегазовых месторождений с помощью АСОДУ и АСУТП позволяют значительно повысить эффективность, безопасность и надежность производственных процессов, а также улучшить управление технологическими операциями.

Автоматизация бурения нефтяных и газовых скважин оптимизирует процессы, повышает безопасность и увеличивает производительность за счет применения современных технологий. Внедрение автоматизированных систем позволяет снизить производственные за-

траты и улучшить эффективность, обеспечивая рациональное использование ресурсов.

Этапы автоматизации бурения нефтяных и газовых скважин

Первый этап включает разработку и проектирование оборудования и программного обеспечения, с учетом всех особенностей и требований для бурения в различных условиях и на разных глубинах.

На втором этапе осуществляется внедрение автоматизированных систем управления процессом бурения. Это включает установку датчиков, программируемых контроллеров и исполнительных механизмов, а также разработку алгоритмов управления на основе данных, получаемых от этих датчиков.

Третий этап предполагает обучение персонала и проведение испытаний технологических систем. Важно убедиться, что все компоненты системы работают корректно и соответствуют требованиям безопасности.

Четвертый этап – эксплуатация и управление (диспетчеризация). Регулярное техническое обслуживание оборудования, контроль его работы и корректировки алгоритмов управления являются ключевыми задачами на этом этапе.

Пятый этап заключается в развитии и модернизации автоматизированных систем бурения с учетом новых технологий и требований рынка. Это включает разработку новых алгоритмов управления и модернизацию существующего оборудования.

Таким образом, автоматизация бурения нефтяных скважин повышает эффективность процессов, снижает производственные затраты и обеспечивает более безопасную и экологичную добычу нефти и газа. Для успешного внедрения систем необходимо учитывать множество факторов, включая особенности местности, специфику месторождения, требования безопасности и экономические аспекты.

2.7. Мониторинг и управление механизированным фондом скважин

С начала интенсивного развития нефтегазовой отрасли и по сегодняшний день основным способом мониторинга механического фонда скважин является периодический обход и осмотр скважин оператором по добыче нефти и газа. При этом оператор производит измерение динамического уровня, отбор проб, снимает показания буферного, линейного и затрубного давлений с помощью манометров, а

также считывает данные со станции управления. Только после этого оператор отвозит пробы в лабораторию, а остальные данные передает технологу. Данный процесс занимает достаточно длительное время, в результате чего не происходит оперативного управление режимами работы скважин, что приводит к дополнительным потерям добываемого флюида.

Одним из важных составляющих интеллектуальных месторождений является удаленный мониторинг и управление механизированным фондом скважин. Мониторинг выполняет несколько организационных функций.

Во-первых, он позволяет определить критические или находящиеся в состоянии изменения явления окружающей среды, в отношении которых необходимо разработать комплекс действий.

Во-вторых, организовывает обратную связь в сфере определенных действий или программ, выявляя причины ранее произошедших положительных и отрицательных результатов, сложившихся в итоге проведения этой программы.

В-третьих, мониторинг устанавливает соответствия правилам и контрактным обязательствам. Процесс управления обычно представляют как последовательные или параллельные действия субъекта, направленные на достижение определенной цели, с возможностью внесения корректировок в процесс работы.

Основными функциями управления является сбор и обработка данных о ресурсах и процессах, постановка и выбор цели, анализ, систематизация, синтез полученной информации со скважин, оптимизация этапов и скорости достижения цели, определение способов и последовательности выполнения задач, организация процессов и контроль способов их выполнения.

Процесс управления может быть как воздействием извне, так и самоуправлением. В первом случае происходит прямое управление объектом в процессе его работы, а самоуправление подразумевает работу объекта в необходимом режиме без прямого вмешательства в этот процесс других объектов.

В настоящее время 85 % добываемой нефти приходится на ЭЦН или комплекс УЭЦН, в который входит и станция управления ЭЦН (СУ ЭЦН). От работы СУ ЭЦН зависит и долговечность оборудования, и правильность работы системы «пласт – скважина – насосная установка». Общая схема устройства мониторинга за работой УЭЦН приведена на рис. 2.19.

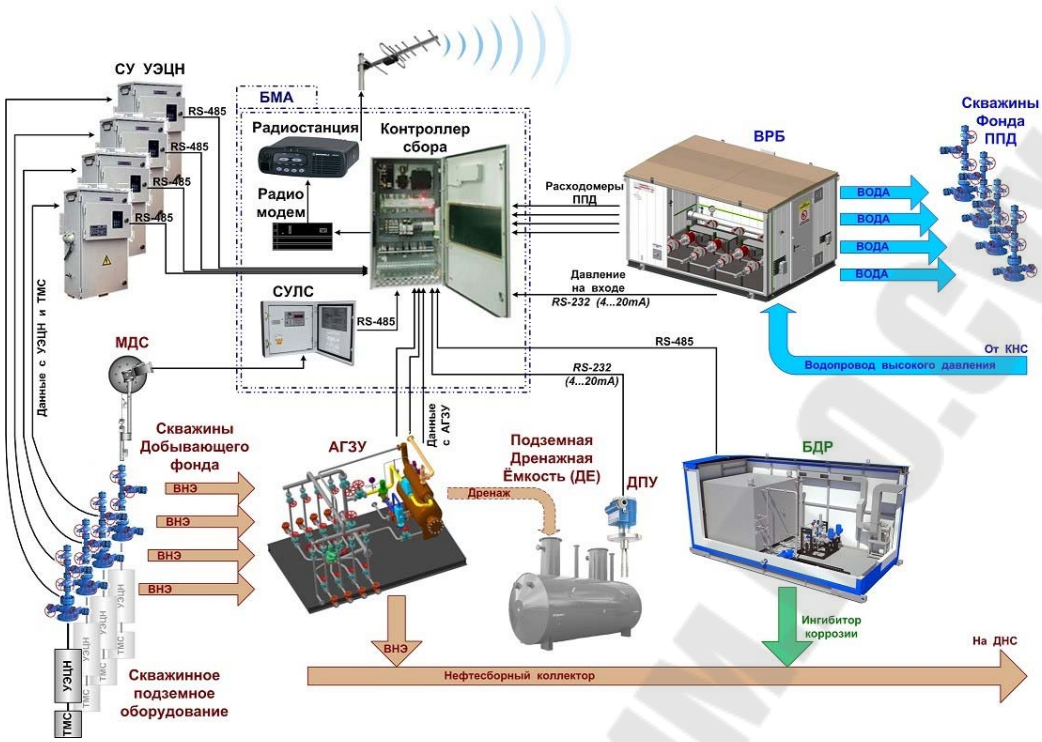

Рис. 2.19. Общая схема устройства мониторинга за работой УЭЦН

Данные станции позволяют производить не только управление, но и мониторинг ЭЦН. Основными их функциями являются:

– обеспечение необходимой защиты насосной установки;

– организация технологического режима работы скважины;

– сбор и передача информации в системы телеметрии;

– хранение истории работы станции управления.

Основным элементом станции управления является контроллер, способный обеспечить выполнение всех вышеперечисленных функций.

Параллельно с этим в нефтегазовой отрасли началось внедрение автоматизированных компьютерных технологий. Однако сегодня данные разведки, добычи, переработки и сбыта все чаще обрабатываются с помощью мобильных приложений, которые позволяют воспользоваться преимуществами облачных вычислений и сетей. Дальнейшее развитие компьютерных технологий позволило расширить объем информации о процессах добычи нефти механизированным способом.

Для структурирования полученной информации, выявления общих закономерностей в процессах, происходящих в определенных условиях, а также прогнозирования дальнейшего развития этих процессов в нефтегазовых компаниях и научно-исследовательских институтах начали создаваться специальные программные комплексы.

В настоящее время все крупные мировые нефтегазовые компании разрабатывают и внедряют в свои процессы производства технологии цифрового мониторинга с применением мобильных устройств. Вся информация о качестве работы механизированного фонда скважин и в целом о разработке месторождения обрабатывается и с помощью специальных приложений передается и выводится на экраны мобильных устройств в реальном времени. Мобильность сбора и анализа информации позволяет обеспечивать круглосуточный контроль и оперативность в принятии решений.

Для создания непрерывного потока информации о работе и состоянии месторождения и его отдельных компонентов необходимо соединить имеющиеся технологии измерения, мониторинга и управления в режиме реального времени, что позволит оперативно реагировать на ситуацию и принимать оптимальные решения.

Главные компоненты данной системы – умные или «интеллектуальные» скважины, в основные функции которых входит непрерывный сбор и анализ всех данных о себе и окружающей среде, на основе которого происходит коррекция технологических режимов работы.

По подсчетам экспертов, внедрение таких скважин позволяет уменьшить себестоимость разработки и эксплуатации месторождения приблизительно на 20 %. Сейчас все нефтегазовые компании стараются активно разрабатывать и внедрять в практику умные скважины (рис. 2.20).

Рис. 2.20. Концептуальная модель интеллектуальной станции управления скважиной

По экспертным оценкам, комплексное использование ИТ-технологий позволяет нефтяникам повысить коэффициент извлечения нефти на 2–7 % и при этом сократить операционные затраты на четверть.

На сегодняшний день все крупные нефтегазодобывающие компании концентрируются на создании интеллектуальных систем с целью снижения удельных затрат на выработку трудноизвлекаемых запасов нефти и снижения себестоимости добычи путем создания средств и технологий мониторинга и управления, позволяющих получать и обрабатывать информацию о работе погружного оборудования и пластов в реальном времени и на этой основе производить оптимальное воздействие на режим эксплуатации пластов и скважин.

Установлены характерные особенности этих систем, которые включают в себя пять уровней: нижним является уровень сбора и передачи данных о работе скважин, а в верхнем происходит оптимизация работы всего месторождения.

На рис. 2.21 приведена схема пятиуровневой системы мониторинга оснащенных установками погружных электроцентробежных насосов скважин (УЭЦН). На сегодняшний день лучшие мировые системы в автоматизированном режиме обеспечивают решение задач первого, второго и третьего уровней. Также происходит разработка автоматизированных систем для четвертого уровня. Для решения задач более высокого уровня привлекаются проектные группы. Рассмотрим уровни данной системы более подробно.

Рис. 2.21. Модель идеальной системы мониторинга

На первом уровне вся информация, поступающая со станций управления и других источников, таких как погружная и наземная телеметрические системы (ТМС), а также автоматические групповые замерные установки, собирается и передается по каналам связи на контрольный пункт. Несмотря на эффективность и многофункциональность используемых сегодня ТМС, для анализа и управления часто используется только 30 % от принимаемой информации.

На втором уровне происходит накопление поступающей информации из различных источников в единой базе данных, ее сортировка, формирование на их основе отчетов в виде структурированных таблиц и их графическое представление (например, в виде построения графиков давления). Данные системы подготовки отчетности достаточно распространены в современных нефтегазовых корпорациях. Из-за большого числа систем, решающих определенные локальные задачи по созданию отчетностей и управления, появляются проблемы с их стандартизацией и унификацией. Для нивелирования данного фактора создаются системы более высокого уровня.

На третьем уровне – контроля и диагностики – разработанные программные комплексы дают возможность определить скважины с отклонившейся от нормы работой и собрать необходимые данные для их анализа. Для этого происходит обработка поступающей информации для выявления отклонений скважины от нормальной работы. Такие системы являются менее распространенными, и часто подобный анализ проводят вручную с помощью подручных программ. На данный момент на этом этапе также реализуется возможность удаленного управления оборудованием скважины, таким как электроцентробежный насос, задвижки и штуцера.

На четвертом уровне – оптимизации добычи – происходит анализ всей системы «скважина – насосная установка – пласт». Он позволяет оптимизировать работу скважины, определить оптимальные параметры режима работы для достижения максимальной эффективности добычи нефти. На данном уровне необходима концентрация данных не только о работе оборудования, но и о геофизических исследованиях скважины, а также история ее работы за последние несколько лет. Работа на данном уровне реализуется с участием экспертов и проектных групп и автоматизирована она в незначительной степени.

На верхнем пятом уровне происходит оптимизация разработки всего месторождения. На данном уровне реализуется всеобщий анализ факторов, оказывающих влияние на работу месторождения.

Оптимизация эксплуатации месторождений в режиме реального времени является сложной задачей даже с использованием современных систем мониторинга. Программные комплексы для анализа и управления работой всего месторождения находятся на стадии разработки в различных компаниях. В основном такой анализ выполняется еще на стадии составления проектных документов и его проведение требует значительных временных и экономических затрат.

При мониторинге процессов, происходящих в скважинах механизированного фонда, наблюдение ведется за целым комплексом показателей, характеризующих работу УЭЦН и свойства коллекторов и флюида как раздельно, так и в целом динамику системы «скважина – пласт». Для оптимизации добычи нефти и газа необходимо в идеальном случае непрерывно определять показания таких параметров потока, как температура, давление, обводненность, расход, состав и свойства флюида, динамический уровень и т. д. Также необходимо контролировать работу насоса, которую можно оценить по частоте вращения, уровне вибраций, температуре обмоток двигателя, сопротивлению изоляции.

Одним из значимых показателей, оказывающих влияние на процесс добычи, является давление. В ходе эксплуатации необходимо контролировать устьевое, затрубное и забойное давление. Первые два измеряются с помощью наземных манометров, установленных на устьевой арматуре. Забойное давление измеряется с помощью глубинного манометра или вычислением веса столба флюида в стволе скважины. Величину забойного давления необходимо знать для недопущения образования газовой шапки, поддержания оптимального уровня депрессии на пласт и для определения режима работы пласта в целом.

Контроль за температурой необходим в связи с тем, что она значительно влияет на свойства пластовых жидкостей. В ходе эксплуатации на нефтяные пласты могут оказываться различные методы воздействия на пласт для интенсификации притока, такие как теплофизические, термохимические методы или применение заводнения с использованием холодной воды. Все это приводит к изменению пластовой температуры в продуктивной части скважины относительно пластовых геотермических условий и, как следствие, изменяются условия разработки объектов эксплуатации.

При использовании в качестве *поддержания пластового давления* методов заводнения необходимо систематически производить

комплекс температурных исследований, в который входят определение отклонения от геотерм в нефтяных залежах, мониторинг температуры воды, нагнетаемой в пласт и выделение работающих пластов в скважинах. Данная информация позволяет изучать и контролировать работу всего механизированного фонда скважин. В частности, это позволяет определить техническое состояние обсадной колонны, наличие в ней негерметичности либо плохой цементации скважины.

Измерение температуры в скважине производится с помощью электрических датчиков (термосопротивления, термопары) либо оптических датчиков (волоконно-оптические распределенные линии и точечные брегговские измерители температуры).

Контроль за изменением свойств нефти в ходе разработки осуществляется с помощью различных глубинных пробоотборников. Так, плотность пластовой нефти и воды измеряют с помощью глубинного пиктометра, динамическую вязкость определяют глубинным вискозиметром, коэффициент объемной упругости – глубинным экспансиметром, а давление насыщения – глубинным сатуриметром.

Физические свойства нефти в пластовых условиях необходимо учитывать при выборе технологии извлечения нефти из пласта на разных стадиях, а также оборудования для сбора нефти на промыслах [2].

Помимо параметров, характеризующих свойства флюида, необходимо также производить мониторинг работы установки погружного электроцентробежного насоса. От качества контроля и правильности принимаемых решений зависят долговечность работы ЭЦН, продолжительность межремонтного периода скважины и, как следствие, сокращение текущих и капитальных затрат на обслуживание скважин.

Основными компонентами погружной части УЭЦН являются телеметрическая система (ТМС), электродвигатель (ПЭД), гидрозащита (ГЗ), насос (ЭЦН), силовой кабель. От надежности каждого компонента зависит общая наработка на отказ всей установки, а следовательно, стоимость ее обслуживания в сутки. Требования к надежности оборудования погружной части очень высоки, так как в процессе эксплуатации данное оборудование недоступно для обслуживания [3].

Единственный компонент УЭЦН, контролирующий текущие параметры установки, – это станция управления.

Важность контроля за характеристиками УЭЦН и своевременного управления его параметрами становится более видна при рассмотрении статистики по продолжительности межремонтного перио-

да работы. Так, в советские времена межремонтный период скважин составлял около 240 суток, а на сегодняшний день этот показатель составляет более 500 суток. При этом некоторые скважины беспрерывно работают и более 10 лет подряд.

Таким образом, мониторинг всех вышеперечисленных параметров в реальном времени с высокой точностью позволяет адаптировать цифровые модели системы «скважина – пласт» под изменяющиеся условия и на основе этого подбирать оптимальные (с экономической и технологической стороны) варианты для дальнейшей разработки (рис. 2.22). Развитие систем мониторинга и управления направлено в первую очередь на более качественное измерение данных параметров и исключение влияния на них человеческого и других факторов.

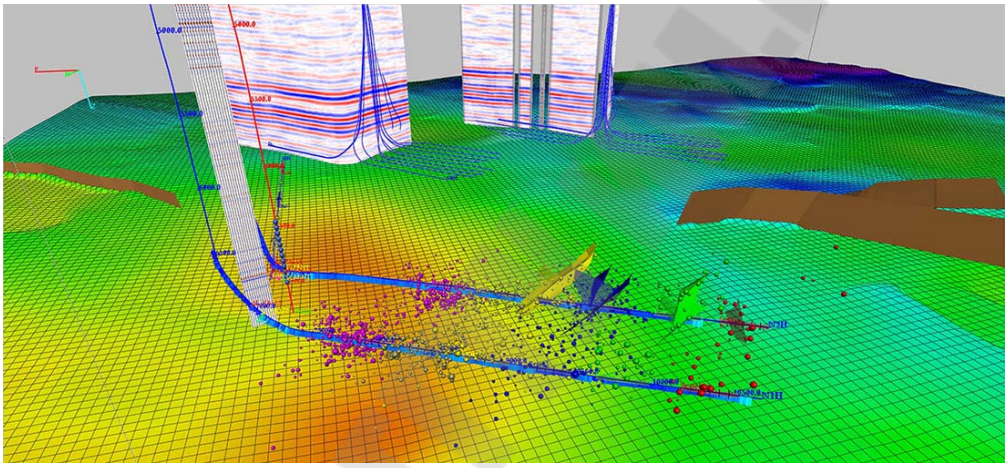

Рис. 2.22. Цифровая модель скважины

Интеллектуальные скважины имеют задачи, которые можно разделить на локальные и общие.

Общие задачи позволяют отслеживать состояние УЭЦН, контролировать расход электроэнергии и получать актуальные данные о параметрах скважины (дебите, давлении, температуры и т. д.). Далее следует анализ собранной информации и оперативное управление параметрами работы. После происходит анализ, обработка, хранение информации и дальнейшее принятие решений об изменении параметров работы системы «скважина – насос – пласт», таких как объемы добычи нефти, расходы на электроэнергию, капитальные и эксплуатационные расходы на работу и других критериев.

Местными задачами являются:

– создание механизмов для дистанционного регулирования рабочих параметров скважины (дебит жидкости, давление, температура,

частота вращения ПЭД и др.) с помощью системы «телеметрическая система – поверхностный внешний прибор – управляющее устройство на объекте разработки»;

– мониторинг работы системы «скважина – насосная установка – пласт» и регулирование этой системы;

– подсчет количества нефти газа и воды, обводненности продукции;

– определение напряжений в колонне НКТ в опасных местах, зависимости потерь в кабеле по стволу скважины;

– мониторинг работы фонда скважин со сложной схемой заканчивания, в которую нельзя погрузить традиционные приборы для геофизических исследований;

– контроль за образованием газогидратных, парафиновых и солевых отложений по длине НКТ, их технического состояния.

Независимо от способа эксплуатации все скважины должны иметь датчики устьевого и затрубного давления, а также температуры жидкости. Желательно оснащение скважин эхолотами для измерения динамического уровня жидкости и расходомерами для контроля дебита.

Скважины, которые эксплуатируются со штанговыми глубинными насосными установками, должны дополнительно быть оборудованы датчиками динамо- и ваттметрирования.

Скважины с электроцентробежными насосами могут оснащаться системами погружной телеметрии, позволяющими контролировать на глубине подвески насосного агрегата такие параметры, как давление и температуру жидкости, уровень вибрации в подшипниках, температуру обмоток погружного электродвигателя, сопротивление изоляции.

Кроме типового набора датчиков, обусловленного особенностями технологического процесса при данном способе эксплуатации скважин, также может возникнуть необходимость в установке дополнительных датчиков, состав которых продиктован особенностями данного месторождения, состоянием оборудования и другими факторами.

При мониторинге скважин с ЭЦН в первую очередь контролируют глубинные параметры с помощью погружной телеметрии, но при этом параллельно наблюдение ведется и наземной телеметрией.

Важной компонентой в мониторинге и управлении скважин с УЭЦН является станция управления. На данный момент создаются интеллектуальные станции управления (ИСУ), способные управлять

работой насоса без участия человека. Основной функцией интеллектуальной станции управления насосной установкой является обеспечение наибольшего дебита нефти в автономном режиме при оптимальных режимах работы насосного и скважинного оборудования и с выполнением иных целевых показателей. В качестве примера существующих в данный момент таких станции можно привести интеллектуальную станциию управления «ОПТИМА» с ПО «GraphIt», предназначенную для графического отображения файлов-отчетов, генерируемых в автоматическом режиме станцией управления ИСУ «Оптима» на экране персонального компьютеров (ПК) (рис. 2.23).

время	глуб.	натяж.	ДВП	Utек	клав	F	режим	ход	(Ошиб)	хеш
14:25:10	0	28.3	не ВП	200	20	1	Полуавтомат	Останов	0	3413
14:25:11	0	28.3	не ВП	228	00	1	Полуавтомат	Останов	0	40AE
14:25:12	0	28.4	не ВП	230	00	1	Полуавтомат	Останов	0	CC49
14:25:13	0	28.4	не ВП	231	100	1	Полуавтомат	Останов	0	C7C2
14:25:14	0	28.4	не ВП	230	100	1	Полуавтомат	Останов	0	AB62
14:25:15	0	28.1	не ВП	229	100	1	Полуавтомат	Останов	0	1075

Рис. 2.23. Рабочий экран rp_graphit_2023.pdf

Данная станция управления позволяет реализовать множество автоматизированных режимов работы за счет наличия алгоритмов адаптации. Всю информацию для работы станция получает от телеметрических систем и других всевозможных датчиков. Интеллектуальная станция управления анализирует поступающие данные и на их основе выбирает алгоритмы действий, наиболее подходящие для той или иной ситуации.

Характерными особенностями интеллектуальных станций управления являются:

– упрощение управления добычей за счет интеграции станции в АСУ верхнего уровня и АСТУЭ: учет и передача телеметрии данных о потреблении электроэнергии в системе кустовой телемеханики;

– самостоятельный вывод скважины на режим и минимизация человеческого фактора при выводе на режим и эксплуатации насосной установки;

– возможность выбора режима работы насосной установки для максимизации дебита;

– автоматическая работа в периодическом режиме, включая мониторинг работы пласта и подбор оптимального времени работы;

– предупреждение аварий, определение их причин, осуществление безопасного запуска насосной установки и, как следствие, уменьшение потерь от простоя скважин из-за аварийных отключений.

Возможности мониторинга интеллектуальных скважин не ограничиваются лишь параметрами, измеряемыми на устье скважины и в ней самой. Для возможности быстрого реагирования на возникающие проблемы на современных скважинах имеются камеры для видеомониторинга.

Современный мониторинг механизированного фонда скважин УЭЦН включает в себя целый комплекс различных датчиков, которые контролируют все параметры работы системы «скважина – насосная установка – пласт». Набор датчиков объединен в общую телеметрическую систему мониторинга, позволяющую собирать информацию по скважине и передавать ее на пульт оператора (рис. 2.24).

Технические требования к системам погружной телеметрии УЭЦН. Данный стандарт является неотъемлемой частью договоров на поставку систем погружной телеметрии УЭЦН. В стандарте помимо базового исполнения ТМС также определены всевозможные опциональные модификации (рис. 2.24). Базовое исполнение ТМС: датчик температуры пластовой жидкости, °С; датчик давления пластовой жидкости, ат; датчик температуры масла ПЭД, °С; сопротивление изоляции, кОм.

ТМС-Н обеспечивает регистрацию параметров давления и температуры пластовой жидкости на выкиде насоса и его использование обеспечивает платформу для создания интеллектуальных алгоритмов управления (определение притока скважины, подачи насоса, установка границ циклов в зоне максимального КПД электроцентробежных насосов и т. д.).

Рис. 2.24. Схема работы программного комплекса
по мониторингу работы механизированного фонда

Системам погружной телеметрии отводится большая роль в качестве инструмента мониторинга и анализа процессов добычи, поскольку ТМС является источником первичной информации и рациональной заменой не только неточным и устаревшим методам теоретических расчетов, но и дорогостоящим мероприятиям по исследованию скважин УЭЦН (рис. 2.25).

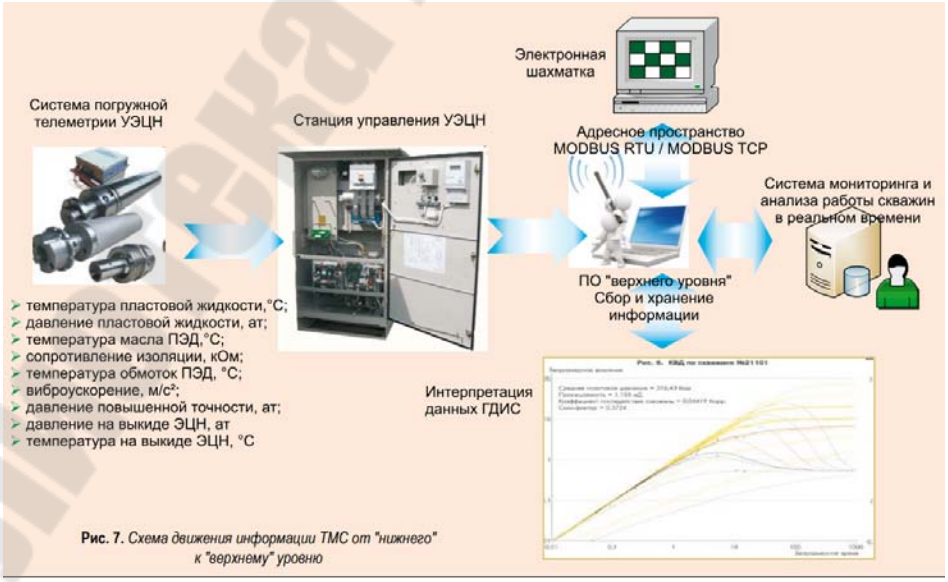

Рис. 2.25. Схема движения информации ТМС от «нижнего»
к «верхнему» уровню

Экономический эффект от применения систем погружной телеметрии типа ТМС-Т может выражаться в снижении капитальных и операционных затрат за счет снижения преждевременных отказов.

2.8. Цифровой двойник скважины с установкой погружных электроцентробежных насосов скважин как средство мониторинга текущей ситуации и прогноза оптимального режима

Цифровой двойник скважины – это программный аналог физического устройства, основанный на математических моделях и позволяющий моделировать внутренние процессы, технические характеристики и поведение в реальных условиях внешних воздействий.

Цифровой двойник процесса функционирования скважины с УЭЦН – это программный аналог скважины со спущенным оборудованием, позволяющий моделировать процессы, возникающие в скважине при работе оборудования. Существующие модели цифровых двойников механизированной скважины могут быть различных видов, каждый из которых имеет ряд недостатков [67]:

1) цифровые двойники, представляющие собой программную реализацию системы математических уравнений, которая описывает течение многофазного потока в элементах скважины и насосного оборудования при заданных управляющих параметрах. Такая модель хорошо интерпретируемая, поскольку описывает физические процессы в скважине, но требует специальной настройки для решения задач по адаптации к фактическим данным и прогнозированию;

2) цифровые двойники, представляющие собой набор алгоритмов для обработки больших объемов данных по технологическому режиму работы скважины с целью получения прогноза на новых параметрах. Такие модели, как правило, не стремятся описать сами физические процессы, а оперируют с откликами системы «пласт – скважина – УЭЦН» на внешние воздействия, поэтому не являются интерпретируемыми и работают по принципу «черного ящика». Их основной недостаток заключается в неверном прогнозе, при котором проанализировать причину такого результата практически никогда не получается.

Цифровые двойники процесса функционирования скважины с УЭЦН, в которых отсутствуют указанные недостатки, должны иметь следующие элементы:

– математическую модель скважины с насосной установкой, включающую модели пласта, элементы скважины (насосно-компрессорная обсадная колонна, затрубное пространство) и насосную установку (насос, ПЭД, кабельная линия и т. д.);

– параметры настройки модели, такие как эффективный коэффициент продуктивности, коэффициент деградации напора и мощности УЭЦН и др.;

– алгоритмы адаптации на замерные значения, в том числе удаление выбросов, сглаживание и экстраполяция;

– алгоритмы прогноза режима работы скважины, в том числе определение возможности достижения целевых параметров после смены насосного оборудования, расчет оптимальной частоты УЭЦН.

В общем случае алгоритм применения цифрового двойника процесса функционирования скважины с УЭЦН состоит из следующих этапов.

Первый этап – цифровой двойник процесса функционирования скважины с УЭЦН начинает функционировать еще до момента кнопочного запуска насоса в работу, с учетом характеристик глубинно-насосного оборудования и параметров скважины производится оценка пластового давления и рассчитывается стартовая частота вращения вала погружного электродвигателя, которая обеспечит подъем продукции скважины до устья без риска срыва подачи по напору. Импорт замерных параметров (дебит, давление на приеме, электрические параметры со станции управления и др.) начинается сразу после кнопочного пуска насоса.

На основе реализованных математических моделей по известным замерным параметрам восстанавливается фактический режим работы скважины. При этом учитывается история изменения замерных параметров, поэтому параметры настройки модели экстраполируются на основе существующего тренда изменения фактического режима работы скважины.

Второй этап – после того, как математическая модель полностью адаптирована на замерные параметры, проводится оптимизация таких параметров, как прогнозная частота тока, длительность периодов работы и остановки УЭЦН (в случае функционирования скважины в режиме периодической эксплуатации) и др., которая позволяет достичь потенциальных значений дебита и забойного давления [67].

Однако существует технологическая сложность и сложность интеграции цифрового двойника с существующими системами предпри-

ятия – это одни из ключевых вызовов при внедрении данной технологии. Они обусловлены рядом факторов:

– *разрозненность данных и систем*: для создания полноценного цифрового двойника требуется объединить огромные объемы данных из разнообразных источников (датчики, SCADA, MES, ERP и др.), которые часто используют разные форматы и протоколы;

– *устаревшее оборудование* (*унаследованные системы*): многие промышленные предприятия используют старое оборудование, не предназначенное для работы с современными цифровыми технологиями. Интеграция с такими системами может потребовать значительных модификаций или установки дополнительных шлюзов и сенсоров;

– *точность и реализм моделирования*: создание виртуальной модели, которая точно воспроизводит поведение и физические свойства реального объекта или процесса в реальном времени, требует сложных алгоритмов, высокопроизводительных вычислений и постоянной калибровки;

– *кибербезопасность*: интеграция множества систем и передача больших объемов данных создают новые уязвимости и риски информационной безопасности, особенно для критической инфраструктуры предприятия;

– *выбор и управление технологиями*: необходимо выбрать подходящие технологии (IoT, ИИ, машинное обучение, облачные вычисления) и управлять их взаимодействием в рамках единой платформы.

Также существует и сложность интеграции с существующими системами предприятия:

– *несовместимость протоколов и интерфейсов*: существующие на предприятии информационные и операционные системы (ОТ и ИТ) часто имеют несовместимые интерфейсы и протоколы обмена данными. «Бесшовная» интеграция требует разработки специальных коннекторов или промежуточного ПО (middleware);

– *различные уровни зрелости систем*: *с*истемы разных уровней (от полевых устройств до ERP) находятся на разных этапах цифрового развития, что усложняет их гармоничное объединение в единую экосистему цифрового двойника;

– *целостность и качество данных*: обеспечение достоверности, непротиворечивости и актуальности данных, поступающих от всех интегрированных систем, является критически важной и сложной задачей. Искажение информации может привести к неверным управленческим решениям;

– *организационные барьеры*: интеграция систем часто требует изменений в устоявшихся технологических и бизнес-процессах, а также вовлечения и обучения персонала из разных отделов (производство, ИТ, управление).

Таким образом, успешное внедрение цифровых двойников требует комплексного подхода, инвестиций в модернизацию инфраструктуры и тщательного планирования интеграционных работ.

2.9. Роботизированная автоматизация

Как показал анализ процессов цифровой трансформации нефтегазовой индустрии, на российском и белорусском рынках широкого распространения роботов не наблюдается по целому ряду причин: нежелание участников рынка нарушать устоявшиеся процедуры; инвестировать в дорогостоящие разработки, отвечающие требованиям рынка; жесткая нормативно-правовая база, регулирующая нефтегазовые операции.

Нефтегазовая промышленность является одной из немногих отраслей, где многомиллиардные затраты на технологические решения не обещают получения прибыли. В основном это связано с усложнением способов добычи нефти: если раньше при геологоразведке обнаруживались насыщенные пласты нефти, то сейчас компании сталкиваются с трудноизвлекаемой нефтью, залегающей в тонких низкопроницаемых пластах. Вскрытие бурением не дает ожидаемого притока, что приводит к необходимости поиска инновационных решений для роста эффективности добычи. Развитие робототехники в средне- и долгосрочной перспективе минимизирует риски для персонала, сократит сроки выполнения операций, ускорит процесс принятия решений с достижением повышенных показателей эффективности в технологических процессах.

Согласно международному стандарту ISO 8373:2012 и национальному стандарту ГОСТ Р 60.0.0.4-2019 [3, 4], *робот* является приводным механизмом, программируемым по двум и более осям, имеющим некоторую степень автономности, движущийся внутри своей рабочей среды и выполняющий предназначенные ему задачи.

Функциональное определение робота можно трактовать как любое устройство (механизм), выполняющее предназначенные ему действия, которое одновременно отвечает трем условиям:

– *воспринимать* окружающий мир с помощью сенсоров (микрофоны, камеры всех областей электромагнитного спектра, различные электромеханические сенсоры и др.);

– *понимать* окружающий мир и строить модели поведения, для того чтобы выполнять предназначенные ему действия;

– *воздействовать* на физический мир тем или иным способом. Если хотя бы одно из этих условий не выполняется, устройство уже нельзя считать роботом.

Роботизация в нефтегазовой индустрии имеет глобальные перспективы. В ближайшем будущем планируется заменить людей, решающих операционные задачи в суровых погодных условиях или отдаленных районах, роботами. Более того, большинство крупных компаний в сотрудничестве с партнерами уже разрабатывают новые роботизированные системы, решая конкретные прикладные задачи.

В настоящее время инженерные решения по роботизации в нефтегазовой отрасли имеют следующие области внедрения:

– роботы-манипуляторы;

– роботы для внутритрубной диагностики;

– инспекционные работы;

– складская робототехника;

– сварочные роботы;

– операции в замкнутых пространствах и опасных зонах;

– оценка качества химического и физического состояния материалов;

– пластовые нанороботы на нефтяных месторождениях;

– подводное и морское глубоководное оборудование.

Для этого используют основные типы роботов:

– *наземные роботы*: применяются для инспекции, технического обслуживания, тушения пожаров и мониторинга оборудования. Например, беспилотники для подготовки строительной площадки на месторождении, буровые установки с автоматическим соединением труб без участия человека;

– *воздушные дроны*: проводят аэрофотосъемку, визуальные проверки трубопроводов и резервуаров, а также выявляют утечки метана с помощью специальных сенсоров и др.;

– *подводные роботы*: обслуживают морские месторождения, проверяют состояние трубопроводов и конструкций на глубине, снижая риски для людей.

Рассмотрим некоторые примеры внедрения робототехнических устройств.

British Petrolium в порядке эксперимента использовал четвероногого робота Spot от Boston Dynamics для мониторинга платформ в Мексиканском заливе (рис. 2.26). Задача инженеров – определить, можно ли с помощью них повысить безопасность и эффективность работы. Робот Spot управлялся дистанционно из офиса Cognite на суше, сделал изображения и сканы, снял показания с датчиков, которые были «удаленно» агрегированы и проанализированы с помощью облачной платформы Cognite Data Fusion. Робот Spot оснащен системой камер для обнаружения препятствий, способен преодолевать сложные маршруты, в том числе передвигаться по лестницам, может нести груз весом 14 кг. Также он может искать места утечек газа и быть «глазами» для удаленных операторов. Эти данные обеспечивают наземным операторам телеприсутствие на морских установках, позволяя им завершить планирование миссий в реальном времени и проводить важнейшие работы.

Рис. 2.26. Четвероногий робот Spot от Boston Dynamics (https://i.pinimg.com/736x/d4/7b/04/d47b04a23f800b97fb2391ffe69519d5.jpg)

Saudi Aramco применяет роботов всех типов – от пожарных до подводных – для инспекций и аварийного реагирования.

В России и Беларуси применяют роботизированные установки пожаротушения, функцией, входящих в ее состав пожарных роботов, является наведение струи на очаг загорания по заданным координатам и тушение очага загорания по заданной площади с заданной интенсивностью орошения. Налажен выпуск роботизированных установок пожаротушения (РУП), представляющих собой комплекс средств автоматической пожарной сигнализации и дистанционно-управляемых лафетных стволов, позволяющий в автоматическом режиме обнаруживать очаг возгорания в его начальной стадии развития, акти-

вировать систему наведения лафетных стволов пожаротушения и подачи огнетушащих средств непосредственно в очаг горения и на защищаемое оборудование.

Отличительной особенностью роботизированных лафетных комплексов является возможность их адаптации к условиям недетерминированного развития аварийной ситуации, тем самым оптимизировать режим тушения, обеспечивая необходимую интенсивность подачи водопенных составов в наиболее опасные технологические зоны без непосредственного присутствия людей (рис. 2.27).

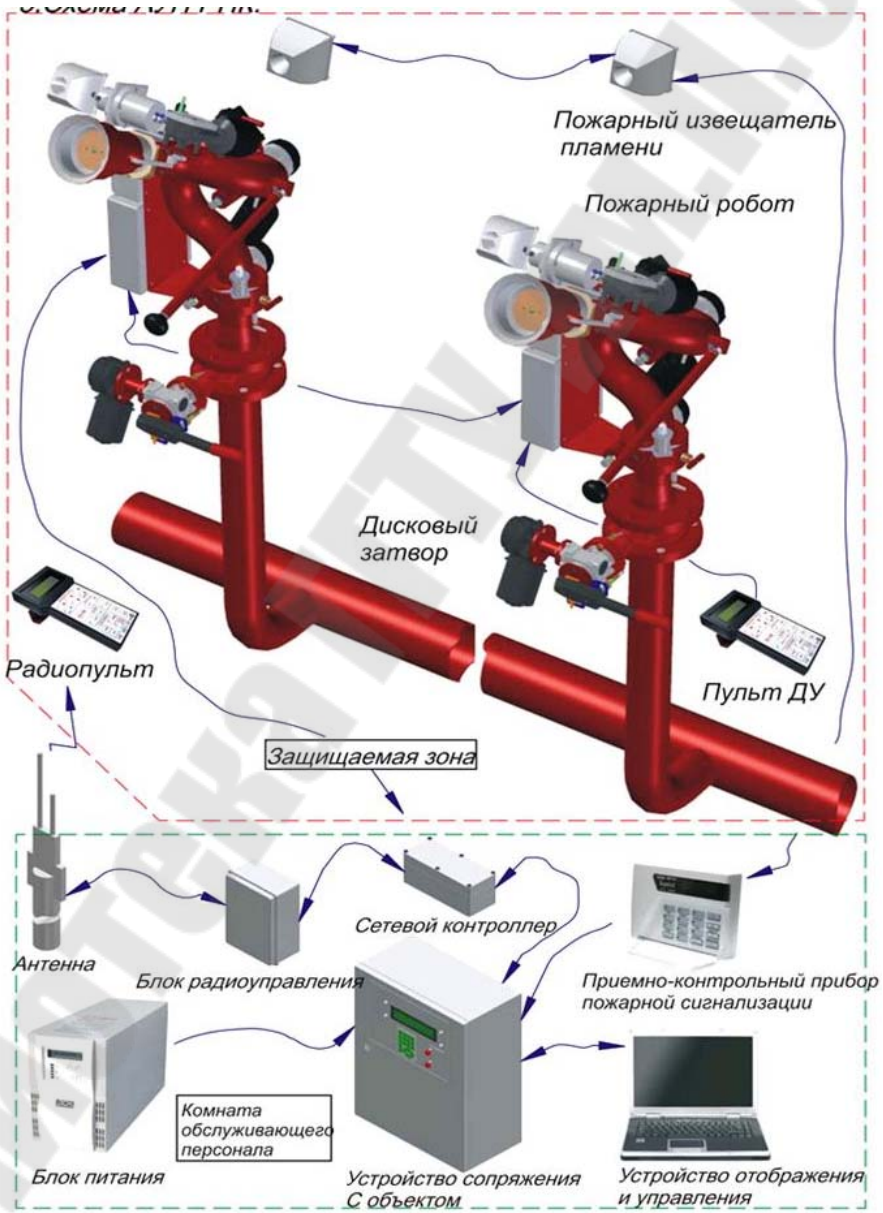

Рис. 2.27. Схема автоматической установки пожаротушения на базе роботизированного комплекса (https://ok-t.ru/studopedia/baza13/816266864771.files/image102.jpg)

«Газпром нефть» (Россия) тестирует автономные строительные площадки с беспилотными бульдозерами и использует 3D-принтеры прямо на месторождениях для изготовления запчастей.

На рис. 2.28 приведен высокоавтоматизированный беспилотный гусеничный бульдозер на базе серийной модели D10 (челябинская компания «ДСТ-Урал»). Управление рядом рабочих операций машины, у которой нет кабины, происходит без участия тракториста. Контролируется бульдозер при помощи планшета. Оператор задает беспилотнику координаты стройплощадки, на которой ему предстоит работать, после чего машина точно следует согласно заданному ей алгоритму движения. Планшетом комплектуется каждый образец. Управлять движением и навесным оборудованием бульдозера также можно по радиоканалу при помощи двух джойстиков дистанционного пульта.

Рис. 2.28. Беспилотный гусеничный бульдозер на базе серийной модели D10 «ДСТ-Урал» на строительной площадке

2.10. Внедрение беспилотных летательных аппаратов

Внедрение *беспилотных летательных аппаратов* (БПЛА, дронов) в деятельность нефтегазовых предприятий ощутимо снижает расходы на контрольные мероприятия по мониторингу безопасного и продуктивного функционирования объектов, а также повышает про-

дуктивность надзорных работ (рис. 2.29). Беспилотники позволяют оперативно собирать необходимые сведения, проникая в труднодоступные места, куда неспособны попасть классическая техника или человек.

Рис. 2.29. Сфера применения беспилотных летательных аппаратов (дронов) в нефтяной отрасли (www.2c05135ca95b0324af6f25af7b419828.jpg (1729×973))

Основные преимущества использования БПЛА в нефтяной и газовой отраслях:

– *повышение безопасности работы*: регулярный контроль за состоянием оборудования и нефтяной системы предотвращает возможные аварии;

– *финансовая выгода*: покупка и эксплуатация беспилотников обходится в десятки раз дешевле применения пилотируемой техники;

– *эффективность работы дронов*: аппараты способны проникать в труднодоступные места. Оборудованные тепловизорами беспилотники выполняют качественные снимки в условиях плохой видимости. Их полет легко регулируется дистанционно (рис. 2.30).

Применение беспилотников оправдано на всех этапах ведения нефтегазовых работ:

• *Предварительная геологическая разведка местности.* Дроны много лет применяются как эффективные инструменты сбора топографических данных. Оборудованные высококачественной фото- и видеотехникой аппараты позволяют получить полную и качественную информацию об интересующем участке с дальнейшим составлением ортофотопланов, 3D-моделей местности и др.

• *Управление строительными и ремонтными работами*. Беспилотники повышают эффективность мониторинга строительных работ на месторождениях. Благодаря высоким техническим характеристикам аппаратов надзор можно автоматизировать.

• *Обследование инфраструктуры.* Использование БПЛА для обследования оборудования нефтегазового сектора является экономически выгодным и результативным решением. Беспилотник снимает изображения высокого качества во время полета. Полученные данные становятся материалом для анализа и оценки системы коммуникаций и прилегающей территории.

Рис. 2.30. Запуск дрона для обследования территории месторождения

Беспилотный аппарат обнаружит несанкционированные врезки в трубопровод, не предусмотренные проектом. Благодаря данным, полученным в режиме реального времени, работники нефтегазовой системы предскажут или выявят и устранят разливы, утечки, коррозию и прочие повреждения трубопровода (рис. 2.31).

• *Инвентаризация и планирование.* Инвентаризация поддерживает актуальность базы данных об объектах, используемом оборудовании и общей территории комплекса. Беспилотные летательные аппараты создают снимки изменений местности, выявляют наличие строящихся объектов и предотвращают хищение имущества. Точные результаты инвентаризации избавляют от неожиданных поломок и торможения процесса нефте- и газоснабжения, позволяют планировать бюджет на ремонт, исходя из регулярно обновляемых сведений.

• *Охрана территории*. Регулярные полеты беспилотников проводят мониторинг территории объекта от проникновения на него посторонних лиц.

Рис. 2.31. БПЛА в процессе обследования трубопровода

• *Возможность быстрого реагирования* в условиях внештатных ситуаций. Дроны собирают и передают информацию в кратчайшие сроки, что позволяет принимать оперативные решения по устранению проблем.

• *Обследование факелов* – ключевой способ применения беспилотников в нефтегазовой промышленности. В основе работы дронов – сбор топографических данных для последующего создания 3D-моделей с целью проектирования возможных аномалий в функционировании буровой системы.

Основные преимущества БПЛА:

– оперативность сбора данных;

– проверка факелов без приостановки работы аппаратуры;

– контроль дефектов в динамике. Дроны выполняют высококачественные снимки в любых ракурсах и проекциях, что позволяет отслеживать малейшие изменения в состоянии оборудования.

Например, российская разработка научно-производственного центра ПЕРГАМ – дистанционный лазерный детектор (ДЛД) метана – предназначена для обнаружения мест утечек природного газа, измерения концентрации облака метана в атмосферном воздухе. Дистанционный лазерный детектор автоматически сигнализирует о превышении концентрации газа заданного порогового значения (рис. 2.32). Детектор измеряет суммарную концентрацию газа в луче лазера, который отражается топографическим объектом (земля, трава, деревья, асфальт, кирпич и т. д.), находящимся на расстоянии 20–150 м от прибора (https://www.pergam. ru/articles/detektor-metana-avia.htm).

• *Быстрая обработка информации с наглядными результатами*. Полученные дроном сведения обрабатываются программным

обеспечением автоматически. Результаты представлены в виде графического отчета, где каждый дефект отмечен отдельным цветом.

• *Поиск утечек нефти.* Регулярность контрольных полетов беспилотников и способность выполнять качественные снимки вне зависимости от удаленности объекта и условий видимости помогают обнаруживать утечки нефти и газа на самых ранних стадиях. Дрон выполняет съемку камерой высокого разрешения (тепловизором при необходимости), после чего данные обрабатываются и анализируются.

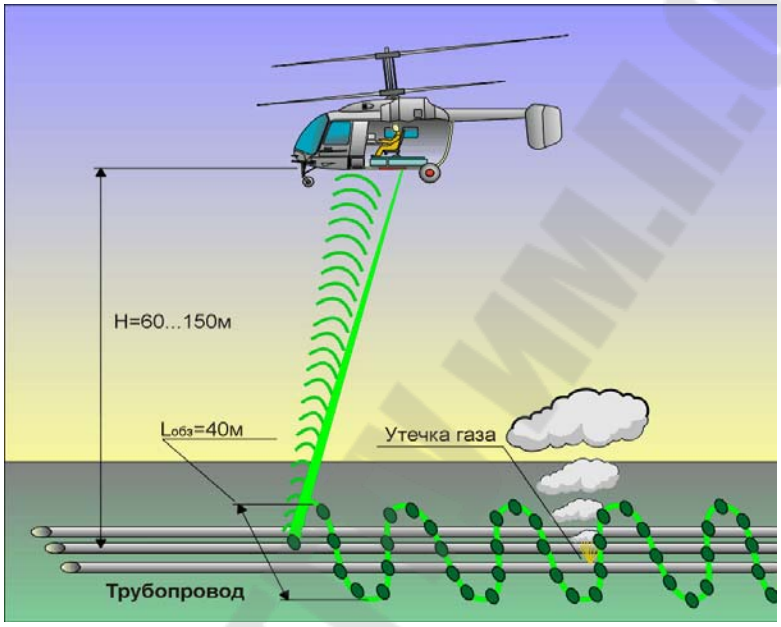

Рис. 2.32. Детектор метана для беспилотного авиационного комплекса (https://www.pergam.ru/articles/detektor-metana-avia.htm)

• *Экологический мониторинг*. Для обследования территории на наличие загрязнения нефтепродуктами и разливов БПЛА передают точные картографические данные, которые помогают: предотвратить негативное воздействие производства и транспортировки ископаемых; определить поврежденный участок; спланировать мероприятия по устранению ущерба экологии.

• *Поиск врезок.* Беспилотники совершают облеты и выявляют самовольные подключения к трубопроводам, помогают в дистанционном режиме контролировать целостность системы и определять правонарушителей.

Таким образом, использование беспилотников как альтернативы традиционным способам контроля помогает снизить затраты в десятки раз.

Глава 3. Инструменты цифровой трансформации

3.1. Машинное зрение

Среди всех направлений ИИ особую востребованность получило машинное (компьютерное) зрение.

Компьютерное зрение (Computer Vision) – это отрасль ИИ, которая использует машинное обучение для быстрой обработки и анализа данных с фотографий или видео. Она включает в себя набор методов, которые наделяют компьютер способностью «видеть» и извлекать информацию из увиденного. Задачи компьютерного зрения приведены на рис. 3.1.

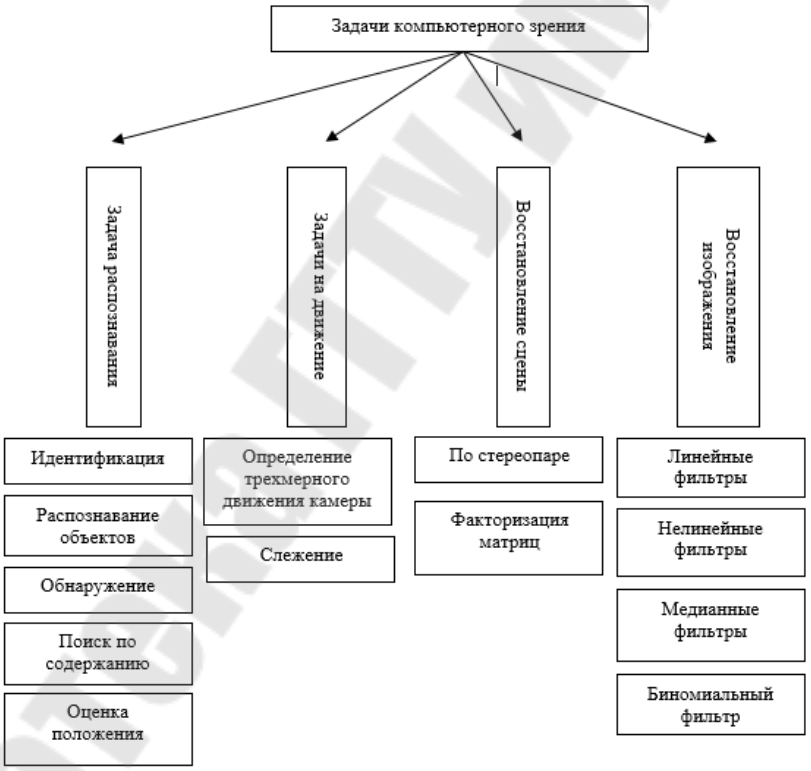

Рис. 3.1. Схема задач компьютерного зрения

Востребованность компьютерного зрения для нефтяной промышленности связана с высокой повторяемостью событий, влиянием человеческого фактора на производственные процессы, ускорением рабочих процессов, а также высоким потенциалом экономического эффекта.

На основе опросов потенциальных заказчиков из нефтяного сектора существует потребность во внедрении компьютерного зрения по следующим запросам на рынке: минимизация выезда на удаленные месторождения; автоматизация сбора данных; детектирование нарушений правил безопасности в режиме реального времени; безопасность и контроль сотрудников на местах добычи, буровых и промышленных зонах. Снижение травмоопасности, повышение дисциплины; аналитика качества хранения; детекция и сегментация дефектов; контроль качества, аналитика объемов использованных строительных материалов; снижение числа ремонтов и времени простоя в местах добычи и на производстве за счет мониторинга и некоторые другие.

Главными областями использования технологий компьютерного зрения в нефтяной промышленности являются: удаленный мониторинг; безопасность; оптимизация и оценка производства; снижение затрат на производство.

Рассмотрим самые востребованные сценарии использования компьютерного зрения и то, как они уже начали внедряться.

Удаленный мониторинг

Для автономной работы внедряют технологии компьютерного зрения и машинного обучения, которые позволяют удаленно с помощью видео проводить мониторинг рабочего процесса. Системы распознают определенные события и в режиме онлайн 24/7 передают в диспетчерскую, что значительно сокращает физические проверки месторождения.

Основная цель диспетчерской – создание системы видеомониторинга, которая способна обеспечить круглосуточный контроль периметра территории, камер для выявления чрезвычайных ситуаций, контроля въезда и выезда транспорта, распознавания номера машин, оповещения о несанкционированном доступе, наблюдения за действиями персонала на объекте, соблюдения правил промышленной безопасности и др.

Для этого требовалось создать удобную систему, которая позволит:

– выводить видеопотоки с камер наблюдения на видеостену;

– управлять раскладками экранов;

– настраивать отображение под текущие задачи.

Решение должно интегрироваться в корпоративную сеть нефтедобывающего предприятия, соответствовать требованиям информационной безопасности и обеспечивать бесперебойную работу даже в случае сбоев электропитания.

Интегрированный программно-аппаратный комплекс в виде интерактивной системы видеоконтроля в диспетчерской решает следующие ключевые задачи:

– сбор и объединение видеосигналов;

– вывод аудио и видео на видеостену;

– оперативное реагирование на сбои;

– круглосуточный контроль состояния оборудования.

Основа видеостены обычно состоит из нескольких профессиональных панелей, установленных в требуемой конфигурации. Панели обеспечивают высокое качество изображения, равномерную яркость и надежную работу, что критично для круглосуточного наблюдения за объектом.

Центральный элемент системы – контроллер видеостены, объединяющий видеосигналы с рабочих станций, сервера видеонаблюдения и ТВ-тюнера. Система должна поддерживать гибкое управление раскладками: диспетчеры могут использовать предустановленные пресеты (пресет – это своего рода фильтр для фотографий с набором настроек) или создавать свои конфигурации.

Управление звуком и электропитанием, мониторинг состояния сети в реальном времени, а также быстрое переключение между источниками сигнала организовывается на базе системы управления, включающий процессор с двумя интерфейсами: переносным планшетом для мобильного контроля и стационарной сенсорной панелью.

Аудиоподсистема позволяет воспроизводить звук с подключенных к контроллеру источников. Надежную связь между компонентами обеспечивает сетевое оборудование, являющееся связующим оборудованием и позволяющее организовать корректную работу системы управления.

Безопасность

Рабочая среда на объектах нефтяной промышленности, воздействие высоких температур и токсичных паров может быть опасна для жизни сотрудников. Любое несоблюдение стандартов безопасности может привести к травмам и серьезным штрафным санкциям. С помощью компьютерного зрения можно нивелировать эти ситуации.

Видеоаналитика позволяет: распознавать средства индивидуальной защиты (СИЗ); осуществлять трекинг людей и объектов, контроль опасных зон, аналитику поведения сотрудников; соблюдать условия пожарной безопасности; обнаружить утечки и др.

Например, для обнаружения утечки используется компьютерное зрение с программным обеспечением, которое использует камеры,

подключенные к Интернету, для наблюдения за буровыми площадками и промысловыми объектами на предмет утечек метана или потенциальных нарушителей.

Специальные компьютерные программы распознают определенные события, сотрудники в диспетчерской на местах получают потоковое видео состояния рабочего процесса. При внедрении на месторождениях это программное обеспечение сокращает физические проверки до 50 %.

При подключении к камерам с использованием тепловизора программное обеспечение отправляет предупреждения, когда видны выбросы метана из резервуаров для хранения. В настоящее время ведется работа по расширению этой возможности на летучие выбросы с гораздо меньшими объемами от устьев скважин или компрессорных станций.

Изображение автоматического теплового обнаружения утечек в скважинах и резервуарах для хранения – лишь одно из нескольких приложений на нефтяных месторождениях, обеспечиваемых алгоритмами компьютерного зрения.

Также компьютерное зрение стали внедрять для распознавания СИЗ на работниках.

На участках разработки нефтяных месторождений и нефтеперерабатывающих заводах есть высокая вероятность травматизма из-за пренебрежения техникой безопасности и отсутствия на работниках СИЗ перед входом в опасную зону. К СИЗ относятся такие предметы, как каски, перчатки, защитные очки и одежда повышенной видимости, которые защищают работников от потенциальных опасностей. Отсюда жесткие требования к ношению СИЗ. Из-за нарушений техники безопасности предприятия терпят многомиллионные убытки, а работники получают травмы, поэтому детектировать такие нарушения нужно систематически и как можно раньше. Для обеспечения безопасности сотрудников обученный алгоритм анализирует локацию и отправляет предупреждения в случае отклонения, если работник вышел без средств индивидуальной защиты.

Машинное зрение упрощает обнаружение СИЗ, используя распознавание объектов для автоматического определения того, надеты ли на работниках необходимые средства защиты. Обрабатывая в реальном времени видеопоток с камер, расположенных по всему объекту, алгоритмы распознают, носят ли сотрудники каски, защитные очки, перчатки и другую экипировку. Если работник появляется в

опасной зоне без СИЗ, система может отправить уведомление ответственным лицам или вывести предупреждающее сообщение на мониторы.

Рис. 3.2. Пример обнаружения СИЗ на сотрудниках предприятия (https://www.ultralytics.com/ru/blog/ai-in-oil-and-gas-refining-innovation)

Обнаружение несанкционированного доступа. Анализ видео с камер помогает выявлять проникновение в запрещенные или опасные зоны. Например, если сотрудник без допуска входит в зону хранения опасных веществ, система может автоматически отправить сигнал охране.

Выявление опасных действий и ситуаций. Искусственный интеллект способен обнаруживать падения работников, длительное неподвижное состояние, которое может свидетельствовать об инциденте, или нахождение людей в потенциально взрывоопасных местах. Также система фиксирует опасные манипуляции с оборудованием, например, приближение к работающим механизмам без отключения их питания (https://trends.rbc.ru/trends/industry/67bed8129a7947a7ac9b1594?from=copy).

3.2. Технологии работы с большими данными

Нефтегазовый сектор известен своей способностью адаптироваться под новые требования современного мира, в том числе инфор-

мационных технологий. Доходность активов становится труднее предсказать, наиболее эффективным инновационным подходом для решения этой проблемы можно обозначить технологию больших данных (BigData).

Большие данные (англ. *big data*) в информационных технологиях – серия подходов, инструментов и методов обработки структурированных и неструктурированных данных огромных объемов и значительного многообразия для получения воспринимаемых человеком результатов, эффективных в условиях непрерывного прироста, распределения по многочисленным узлам вычислительной сети, альтернативных традиционным системам управления базами данных и решениям класса Business Intelligence. В данную серию включают средства массово-параллельной обработки неопределенно структурированных данных, прежде всего, решениями категории NoSQL, алгоритмами MapReduce, программными каркасами и библиотеками проекта Hadoop.

К *большим данным* относят информацию, чей объем может быть свыше сотни терабайтов и петабайтов. Причем такая информация регулярно обновляется. В качестве примеров можно привести данные, поступающие от многочисленных датчиков с нефтяных или газовых месторождений, и т. п. Также в понятие «большие данные» иногда включают способы и методики их обработки.

Если же говорить о терминологии, то Big Data подразумевает не только данные как таковые, но и принципы обработки больших данных, возможность дальнейшего их использования, порядок обнаружения конкретного информационного блока в больших массивах. Существуют критерии информации, которые позволяют оценить, соответствуют ли данные понятию Big Data или нет.

В качестве определяющих характеристик для больших данных отмечают «три V»:

– объем (англ. *volume*, в смысле величины физического объема);

– скорость (англ. *velocity*, в смысле как скорости прироста, так и необходимости высокоскоростной обработки и получения результатов);

– многообразие (англ. *variety*, в смысле возможности одновременной обработки различных типов структурированных и полуструктурированных данных).

В качестве примеров источников возникновения больших данных приводятся непрерывно поступающие данные с измерительных устройств, события от радиочастотных идентификаторов, потоки со-

общений из социальных сетей, метеорологические данные, данные дистанционного зондирования Земли, потоки данных о местонахождении абонентов сетей сотовой связи, устройств аудио- и видеорегистрации.

Методы и техники анализа, применимые к большим данным:

– методы класса Data Mining: обучение ассоциативным правилам (англ. *association rule learning*), классификация (методы категоризации новых данных на основе принципов, ранее примененных к уже наличествующим данным), кластерный анализ, регрессионный анализ;

– краудсорсинг – категоризация и обогащение данных силами широкого, неопределенного круга лиц, привлеченных на основании публичной оферты, без вступления в трудовые отношения;

– смешение и интеграция данных (англ. *data fusion and integration*) – набор техник, позволяющих интегрировать разнородные данные из разнообразных источников для возможности глубинного анализа, в качестве примеров таких техник, составляющих этот класс методов, приводится цифровая обработка сигналов и обработка естественного языка (включая тональный анализ);

– машинное обучение, включая обучение с учителем и без учителя, а также *Ensemble learning* (англ.) – использование моделей, построенных на базе статистического анализа или машинного обучения для получения комплексных прогнозов на основе базовых моделей (англ. *constituent models*, ср. со статистическим ансамблем в статистической механике) (рис. 3.3);

– искусственные нейронные сети, сетевой анализ, оптимизация, в том числе генетические алгоритмы;

– распознавание образов;

– прогнозная аналитика;

– имитационное моделирование;

– пространственный анализ (англ. *spatial analysis*) – класс методов, использующих топологическую, геометрическую и географическую информацию в данных;

– статистический анализ, в качестве примеров методов приводится A/B-тестирование и анализ временных рядов;

– визуализация аналитических данных – представление информации в виде рисунков, диаграмм, с использованием интерактивных возможностей и анимации как для получения результатов, так и для использования в качестве исходных данных для дальнейшего анализа.

Рис. 3.3. Процесс машинного обучения

Наиболее часто указывают в качестве базового принципа обработки больших данных SN-архитектуру, обеспечивающую массивно-параллельную обработку, масштабируемую без деградации на сотни и тысячи узлов обработки. При этом, кроме рассматриваемых большинством аналитиков технологий NoSQL, MapReduce, Hadoop, R, включает в контекст применимости для обработки больших данных также технологии Business Intelligence и реляционные системы управления базами данных с поддержкой языка SQL.

Существует ряд аппаратно-программных комплексов, предоставляющих предконфигурированные решения для обработки больших данных: Aster MapReduce appliance (корпорации Teradata), Oracle Big Data appliance, Greenplum appliance (корпорации EMC, на основе решений поглощенной компании Greenplum). Эти комплексы поставляются как готовые к установке в центры обработки данных телекоммуникационные шкафы, содержащие кластер серверов и управляющее программное обеспечение для массово-параллельной обработки.

Аппаратные решения для аналитической обработки в оперативной памяти, в частности, предлагаемой аппаратно-программными комплексами Hana (предконфигурированное аппаратно-программное решение компании SAP) и Exalytics (комплекс компании Oracle на основе реляционной системы Timesten и многомерной Essbase), также иногда относят к решениям из области больших данных, несмотря на то, что такая обработка изначально не является массово-параллельной, а объемы оперативной памяти одного узла ограничиваются несколькими терабайтами.

Кроме того, иногда к решениям для больших данных относят и аппаратно-программные комплексы на основе традиционных реляционных систем управления базами данных – Netezza, Teradata, Exadata, как способные эффективно обрабатывать терабайты и экзабайты структурированной информации, решая задачи быстрой поисковой и аналитической обработки огромных объемов структурированных данных.

Аппаратные решения DAS – система хранения данных, напрямую присоединенных к узлам, – в условиях независимости узлов обработки в SN-архитектуре также иногда относят к технологиям больших данных.

Нефтегазовые компании в процессе своей деятельности получают петабайты данных каждый день. Использование больших данных открывает возможности анализа и предсказания развития трендов в области геологии, инженерии, производства и наилучшего способа использования оборудования для достижения наиболее оптимальных результатов работы на всех стадиях своей деятельности, начиная от разведки и добычи и заканчивая переработкой и реализацией готовой продукции. Наиболее успешное применение данной технологии способствует снижению издержек и получению максимальной прибыли за счет использования взаимодополняющих методов предсказания.

Сбор данных может осуществляться не только на стадии добычи и переработки, но и при прогнозировании стоимости продукции, что в целом дает общее представление об оптимизации бизнес-процессов компании для выбора наилучшего производственного цикла и повышает возможности компании на рынке.

Для каждого производственного цикла можно выделить следующие преимущества использования технологии больших данных:

– *разведка* – моделирование и предсказание наиболее вероятных участков добычи с потенциально оптимальными объемами сырья;

– *добыча* – сбор и переработка данных в целях оптимизации использования оборудования и способов добычи;

– *переработка* – улучшение методов и результатов переработки сырья в конечную продукцию в зависимости от цен на рынке, а также для сохранения ресурса перерабатывающего оборудования;

– *транспортировка* – большие данные позволяют выявить потенциальные потребности того или иного сырья в соответствующих регионах, а также выявить наиболее оптимальную нагрузку на средства доставки;

– *реализация* – в данном разделе большие данные способствуют максимальной отдачи при прогнозировании рынка регионов, в целях определения потенциально-прибыльных потребностей в том или ином виде сырья, а также его количества.

Обозначены наиболее общие возможности технологии больших данных в каждом цикле нефтегазовой отрасли. Благодаря большим данным возможно сократить общие издержки компании и превращать нефтегазовую отрасль в наукоемкую, при этом произойдет появление смежных наукоемких отраслей обработки данных и предсказаний, что, в свою очередь, повысит эффективность инновационной деятельности в нефтегазовой отрасли.

3.3. Искусственный интеллект и машинное обучение

Искусственный интеллект – это важная технология, оказывающая влияние на различные сферы нашей жизни. Основы ИИ включают в себя машинное обучение, нейронные сети и обработку естественного языка. Искусственный интеллект находит применение в различных областях, включая робототехнику, автоматизацию процессов и бизнес. Основные алгоритмы ИИ включают в себя алгоритмы машинного обучения и нейронные сети.

Искусственный интеллект – это:

– область компьютерных наук, которая занимается созданием интеллектуальных систем, способных выполнять задачи, требующие человеческой интеллектуальной деятельности;

– совокупность технологических решений, способных имитировать когнитивные функции человека и достигать результатов как минимум сопоставимых с человеческим интеллектом, что также включает в себя способность к самообучению и поиску решений без заранее заданных алгоритмов;

– сложная кибернетическая система, сочетающая компьютерное программное и аппаратное обеспечение с когнитивной функциональной архитектурой и достаточной вычислительной мощностью для выполнения необходимых функций.

В рамках ИИ существует множество технологий и методов, включая машинное обучение и его алгоритмы, нейронные сети, обработку естественного языка.

Машинное обучение – это подобласть ИИ, которая позволяет компьютерным системам обучаться на основе опыта и данных. С помощью машинного обучения компьютерные программы могут само-

стоятельно улучшать свою производительность и адаптироваться к новым задачам.

Алгоритмы машинного обучения – это математические модели и методы, используемые для обучения компьютерных систем на основе данных. С их помощью компьютеры могут находить закономерности в данных, выделять важные признаки и делать прогнозы или принимать решения на основе полученных знаний.

Нейронные сети – это модель, вдохновленная работой человеческого мозга. Они состоят из множества связанных между собой искусственных нейронов, которые обрабатывают информацию и принимают решения на основе полученных данных.

Обработка естественного языка – это сфера ИИ, которая занимается разработкой алгоритмов и моделей, способных понимать и обрабатывать естественный язык, такой как речь или текст. Это позволяет компьютерным системам взаимодействовать с людьми на естественном языке и выполнять задачи, связанные с обработкой текста.

Машинное обучение позволяет ИИ автоматически обрабатывать большие объемы данных, распознавать образы, анализировать тексты и принимать решения. Это открывает много возможностей в различных областях, включая нефтегазовую отрасль.

Однако глубокое обучение – это еще более мощный шаг в развитии ИИ. Это подраздел машинного обучения, который использует искусственные нейронные сети для эмуляции работы человеческого мозга. Глубокое обучение позволяет создавать модели ИИ, которые способны распознавать сложные образы, работать с естественными языками и предсказывать результаты на основе огромного объема данных.

Рассмотрим применение методов машинного обучения для автоматизации процессов в нефтегазовой отрасли.

Классическая автоматизация (КА) в виде математического аппарата основана на математической и имитационной модели с предоставлением физических процессов в режиме реального времени и содержит, как правило, ограничения, связанные с невозможностью распознавания образов.

Современная автоматизация основана на применении методов машинного обучения, которые в результате математических расчетов обученной модели позволяют идентифицировать и классифицировать объекты с распознаванием образов для принятия решений с заданным алгоритмом выполнения процессов и задач.

Машинное обучение и ИИ используются для создания моделей прогнозирования и оптимизации производственных процессов. Одной из основных задач, решаемых с помощью машинного обучения в нефтегазовой промышленности, является контроль и управление состоянием эксплуатационного оборудования. С помощью машинного обучения можно предсказывать возможные отказы оборудования, определять оптимальные режимы работы оборудования, проводить мониторинг состояния оборудования и его диагностику в режиме реального времени [35, 36].

Также машинное обучение может использоваться для прогнозирования потребности в нефти и газе на основе исторических данных и прогнозов спроса. Эти модели могут помочь компаниям оптимизировать производство и управлять запасами эффективнее.

Кроме того, машинное обучение может применяться для управления технологическими процессами в разведке и бурении для нефтедобычи. С помощью алгоритмов машинного обучения можно оптимизировать процессы бурения скважин, улучшить прогнозирование свойств пласта и определять оптимальные параметры эксплуатации нефтяных месторождений [37].

Нефтегазовый сектор, включающий современную автоматизацию, состоит из целого комплекса технологических процессов, которые в результате позволяют получить данные о количестве добытого сырья на основе прогнозирования для выполнения сопутствующих технологических операций – переработки, хранения, транспортирования, прогноза прибыльности и рентабельности на уровне мирового рынка. Современная автоматизация имеет возможность одновременно контролировать и управлять оборудованием, средствами и устройствами для возможности проведения технологических процессов. Важным условием концепции современной автоматизации является составление рисков, объясняемых столкновением с возможными проблемами, которые могут негативно отразиться на выполнении связывающих процессов [39].

Цифровизация производства является эффективным решением для внедрения интеллектуального вида автоматизации, что на сегодня обусловлено интенсивным применением продвинутых интеллектуальных систем и оптимизацией в режиме реального времени. Это способствует анализу больших данных (DataMining) и включает в себя получение данных, интеллектуальный и глубинный анализ данных. Некоторые алгоритмы машинного обучения используются в области

разработки месторождений, которые подпадают под классификацию контролируемого обучения [10]. Большинство реализаций разработок месторождений зачастую используют методы эволюционной оптимизации, например, генетический алгоритм и оптимизацию роя частиц. Краткое описание некоторых алгоритмов приведены в табл. 3.1.

Таблица 3.1

Алгоритмы машинного обучения

Алгоритм	Описание
Логистическая регрессия	Модель, используемая для бинарной классификации, основанная на логистической функции
Решающие деревья	Метод, использующий иерархическую структуру для принятия решений на основе последовательности вопросов
Случайный лес	Модель, объединяющая несколько решающих деревьев для улучшения точности и стабильности предсказаний
Сверточные нейронные сети	Нейронные сети, используемые для анализа и обработки изображений и связанных с ними задач
Рекуррентные нейронные сети	Нейронные сети, которые могут обрабатывать последовательности данных и сохранять информацию о предыдущих состояниях

Нейронные сети – это модели, основанные на структуре и функционировании биологических нервных систем. Они состоят из искусственных нейронов, которые связаны между собой и передают информацию друг другу. Нейронные сети используются для решения задач, требующих обработки и анализа сложных и больших объемов данных, таких как распознавание образов, обработка естественного языка и прогнозирование.

В развитии и применении ИИ возникают различные этические вопросы, требующие серьезного обсуждения и регулирования. Присутствие ИИ в нашей жизни может повлечь за собой негативные последствия и нарушения этических принципов.

Одним из ключевых вопросов является вопрос прозрачности и объяснимости алгоритмов ИИ. Когда ИИ принимает решения, основанные на сложных алгоритмах и нейронных сетях, нам важно понимать, как эти решения принимаются и какие факторы влияют на результаты.

Другой важный вопрос – этическое использование данных. Собирание и использование больших объемов данных позволяет ИИ обучаться и принимать решения. Однако сбор и использование чувствительных персональных данных без согласия людей может нарушать их право на приватность и конфиденциальность.

Также следует обратить внимание на ответственность за действия ИИ. Если ИИ делает ошибку или принимает неправильное решение, кто несет ответственность? Какие меры предусмотрены для предотвращения негативных последствий?

Наконец, следует обсудить вопросы справедливости и дискриминации. Искусственный интеллект может быть подвержен предвзятости, основанной на неравных условиях и неправильной классификации данных. Это может привести к дискриминации и искажению результатов.

Решение вопросов этики в разработке и применении ИИ становится все более важным на фоне быстрого технологического прогресса. Необходимо создать правовые и этические рамки, регулирующие использование ИИ с целью минимизации возможных негативных последствий и обеспечения справедливого и ответственного подхода.

Вызовы ИИ:

– *недостаток качественных данных*: ИИ требует большого объема высококачественных данных для эффективного обучения и принятия решений. Однако иногда такие данные могут быть недоступны или их сбор может быть затруднен;

– *человеческий фактор*: ИИ может столкнуться с трудностями в распознавании и анализе контекста, эмоций и намерений людей. Понимание и взаимодействие с человеком остаются сложными задачами для ИИ;

– *этические вопросы*: возрастает необходимость решения этических вопросов, связанных с применением ИИ. Все больше обсуждается вопрос о том, где проходит грань между полезным использованием ИИ и нарушением прав человека, приватности и безопасности.

Ограничения ИИ:

– *ограниченность обучения*: ИИ, основанный на машинном обучении, может столкнуться с ограничениями, связанными с обучающими данными. Он может оказаться неправильно обученным, если данные содержат искажения или предвзятость;

– *неопределенность и неясность*: ИИ может иметь трудности в объяснении своих решений и принятых выводов. Это создает ограни-

чения в понимании и отслеживании причинно-следственных связей в решениях, принятых ИИ;

– *вычислительные ограничения*: разработка ИИ требует значительных вычислительных ресурсов и мощностей для обучения и выполнения сложных задач. Это может быть ограничением для распространения ИИ.

Ограничения и вызовы ИИ являются стимулом для развития новых методов, алгоритмов и технологий, чтобы преодолеть эти проблемы и раскрыть полный потенциал ИИ.

Проблемы внедрения ИИ в нефтегазовой отрасли

Компьютерное зрение – реализация этого решения для нефтегазовой отрасли сопряжена с некоторыми препятствиями. Одна из главных проблем – получение чистых изображений, на основе которых ИИ сможет обучаться. Окружающая среда в этой отрасли, например, буровые установки, может быть грязной, плохо освещенной и постоянно меняющейся, что делает размытые или непоследовательные кадры непонятными для систем компьютерного зрения.

Кроме того, старые системы камер могут быть недостаточно высокой четкости, чтобы улавливать детали, которые необходимы компьютерному зрению для эффективной работы. Модернизация инфраструктуры камер может стать значительной инвестицией.

Работа с конфиденциальными данными, полученными с помощью этих камер, добавляет еще один уровень сложности. Нефтегазовым компаниям нужны надежные меры кибербезопасности, чтобы защититься от потенциальных утечек данных.

Несмотря на то, что существуют проблемы с внедрением компьютерного зрения в нефтегазовой отрасли, ИИ-сообщество активно внедряет инновации для решения этих проблем.

Однако, несмотря на высокий потенциал ИИ, есть определенные сдерживающие факторы.

Компании нефтегазового сектора используют определенные технологии и системы, которые не всегда совместимы с новыми ИИ-решениями. Чтобы все получилось, нужно модернизировать инфраструктуру и интегрировать ИИ – это длительный и дорогостоящий процесс. Требуются значительные инвестиции в разработку и оптимизацию решений, приобретение вычислительных мощностей и обучение персонала. Для многих компаний, особенно в условиях нестабильных цен на нефть, такие расходы могут быть неподъемными.

Еще один барьер заключается в нехватке квалифицированных специалистов. Чтобы использовать ИИ, нужны люди, которые глубоко разбираются как в технологиях, так и в нефтегазовой отрасли.

Требуется тщательное тестирование технологий. Сложность процессов отрасли наряду с высокими требованиями к безопасности диктует полагаться на проверенные методы. В некоторых случаях необходимость сертификации ИИ-решений, естественно, замедляет их распространение.

Информации для использования технологий не всегда достаточно. Эффективность ИИ зависит от качества и количества данных, применяемых для его обучения. Однако в нефтегазовой отрасли показатели могут быть разрозненными, неполными или недоступными для анализа, что ограничивает возможности использования алгоритмов.

Разведка и геологоразведка. Искусственный интеллект помогает анализировать большие объемы геологических данных для более точного определения месторождений нефти и газа. Алгоритмы обрабатывают данные сейсморазведки, строят 3D-модели и анализируют сложные геологические структуры. Анализ исторических данных о пластовом давлении, работе скважин и добыче позволяет увеличить извлекаемые запасы на 5–10 %. Учет результатов каротажа (метода исследования скважин, определяющего строение пород и их физические свойства) помогает оценить строение скважины и предсказать риски, например, пескопроявление – процесс, при котором частицы песка попадают в призабойную зону.

«Газпром нефть» использует алгоритмы машинного обучения, чтобы интерпретировать сейсмические данные и создавать геологические модели. Это позволяет находить перспективные участки для бурения.

Оптимизация добычи. Искусственный интеллект помогает оптимизировать процессы добычи. Анализ производственных данных позволяет управлять рисками, снижать затраты и разрабатывать более экологичные технологии. Для этого обрабатываются данные с датчиков и систем наблюдения, позволяющие в реальном времени регулировать давление, температуру и дебит скважин – объем жидкости (нефти, воды) или газа, добываемый за определенный период. Также используются сейсмические и геологические данные для поиска новых запасов, информация о работе скважин для повышения нефтеотдачи, данные мониторинга безопасности и энергопотребления.

В некоторых компаниях внедрены алгоритмы машинного обучения, которые анализируют данные с датчиков, установленных на оборудовании, например, показатели температуры, давления, вибрации. На их основе принимаются решения об оптимальной стратегии бурения, корректно рассчитываются давление, объем закачиваемых

жидкостей и другие параметры. Система повышает эффективность работы, оптимизирует расходы и продлевает срок службы устройств.

В ЛУКОЙЛе ИИ активно применяется для управления разработкой зрелых месторождений. Например, ИТ-система «Управление разработкой зрелых месторождений с применением нейронных сетей» благодаря использованию алгоритмов машинного обучения анализирует взаимосвязь между нагнетательными скважинами (через них закачивается вода или газ для поддержания пластового давления) и добывающими скважинами (из них извлекается нефть или газ), рассчитывает оптимальные режимы их эксплуатации и помогает управлять содержанием воды в добываемой продукции. Это позволяет уменьшить объемы жидкости, извлекаемой вместе с нефтью, что повышает нефтеотдачу и снижает операционные затраты (https://trends.rbc.ru/trends/industry/67bed8129a7947a7ac9b1594?from=copy).

3.4. Система обучения по прецедентам

На сегодняшний день в мире изучено и разрабатывается достаточно большое количество месторождений углеводородов, значительная часть которых приходится на крупные залежи с традиционными коллекторами. Традиционными коллекторами являются нефтегазоносные пласты, их освоение началось еще во второй половине XX столетия. Разработка таких пластов, как правило, не осложнена их геологическим строением или свойствами насыщающих флюидов. Однако постепенное истощение традиционных запасов постоянно требует разведки и освоения новых объектов разработки. Сегодня на смену традиционным коллекторам приходят залежи со сложным геологическим строением, низкопроницаемые объекты трудноизвлекаемых запасов (ТРИЗ), объекты ТРИЗ с высоковязкой нефтью, шельфовые залежи углеводородов и т. п. Разработка подобных объектов требует значительных капитальных затрат, поэтому компании-недропользователи уделяют особое внимание такому проектированию разработки и обустройства месторождений, при котором на самых ранних этапах создаются новые технические, технологические, организационные решения, способные повысить рентабельность нефтедобычи. Сложность изучения нефтегазоносных пластов заключается в наличии неопределенности, а именно нельзя точно изучить свойства объекта в межскважинном пространстве. Знания об объекте разработки всегда пополняются в ходе его эксплуатации. На этапе разведки и пробной эксплуатации перед компаниями стоит задача из-

влечь максимально большой объем знаний, необходимый для того, чтобы оценить перспективы самого объекта, составить проектную документацию и начать реализацию проектного решения. Поиск оптимального проектного решения предполагает рассмотрение множества вариантов разработки и обустройства месторождения. На практике специалисты при поиске решений опираются на прошлый опыт, выбирая известные объекты-аналоги с уже готовыми решениями. Эти решения применяются к новому изучаемому объекту, после чего проводится оценка их эффективности для новых условий. Подбор объекта-аналога – это слабоформализованная процедура, основанная на анализе многих условий и оценке схожести сравниваемых объектов. Результат такой процедуры во многом зависит от опыта и компетентности специалиста или эксперта, который занимается поиском объектов-аналогов. При этом зачастую на поиск тратится значительное время, а полученные результаты не являются гарантированно лучшими среди возможных. В области ИИ для автоматизации поиска и принятия решений на основе аналогий разработан и эффективно используется метод, который получил название вывода решений на основе прецедентов, или, как представлено в зарубежной литературе, case based reasoning (CBR). Он не только позволяет объективизировать процесс отбора объектов-аналогов, но и служит основой для построения баз знаний, а также разработки интеллектуальных советующих систем, которые быстро и с экспертной квалификацией способны находить рациональные решения для вновь возникающих ситуаций и объектов.

Метод CBR используется в качестве инструмента поддержки принятия ключевых решений при моделировании нефтегазовых месторождений.

Метод CBR включает в себя цикл, состоящий из трех основных этапов: поиск и отбор, повторное использование и сохранение (рис. 3.4). Новая задача, проходя по циклу CBR, на каждом этапе взаимодействует с базой прецедентов, которая представляет собой множество прецедентов одного типа с новой задачей. Каждый прецедент CASE представляет собой условие Sit и решение R: CASE = < Sit, R >.

На этапе поиска и отбора происходит выборка из базы прецедентов случая (или случаев), наиболее схожего для новой задачи. Далее производится попытка повторного использования готового решения для новой задачи. На завершающей стадии CBR-цикла производится сохранение нового прецедента в базу для дальнейшего использования.

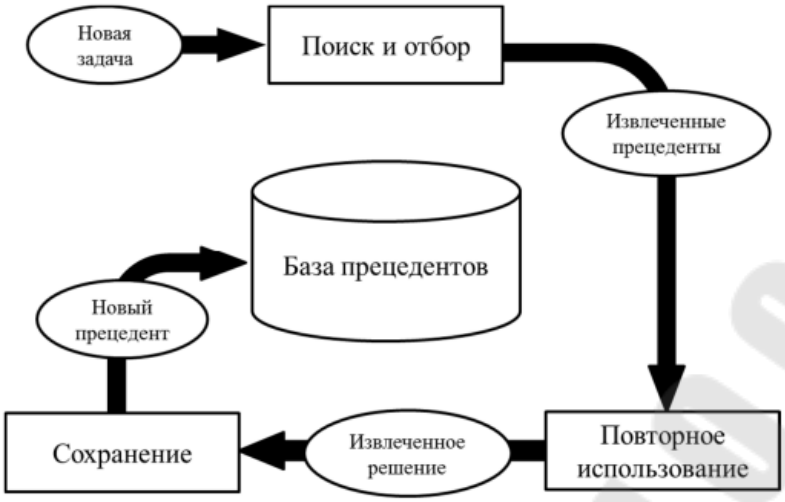

Рис. 3.4. Стадии метода вывода решений на основе прецедентов, CBR-цикла

На сегодняшний день поиск объектов-аналогов остается важным инструментом в практике принятия решений при проектировании разработки нефтяных и газовых месторождений. Выбор объектов-аналогов в значительной степени влияет на принимаемые решения на всех стадиях жизни месторождения. Моделирование месторождений углеводородов является одной из основных частей проектной работы, и решения, принимаемые в ходе моделирования, также зависят от выбора объекта-аналога. Однако сам результат поиска и выбора аналогов во многом зависит от опыта, компетентности и субъективных предпочтений специалистов и экспертов, участвующих в этом процессе.

Предлагаемый подход позволяет минимизировать влияние человеческого фактора, объективизировать процесс принятия решения, поскольку предполагает использование строго формализованной процедуры с количественным обоснованием схожести сравниваемых объектов и рассмотрением всех доступных в базе прецедентов. Последнее является еще одним преимуществом использования CBR-системы, так как при традиционном подходе человеческого ресурса, как правило, не хватает, чтобы произвести исчерпывающий поиск и анализ всех возможных аналогов для принятия решений.

На данный момент уже существует представление о месторождении углеводородов как о прецеденте. Кроме того, инструмент поддержки принятия решений в виде CBR-системы и базы месторождений-прецедентов может быть задействован на всех стадиях проектирования разработки месторождений, где необходим выбор объекта-аналога, а не только при моделировании.

3.5. Облачные решения и системы. Облачные вычисления

Облачные вычисления – это инфраструктура, решения, софт и ресурсы, которые провайдер предоставляет через сеть, точнее – через облако. Это широкое понятие, куда входит vCPU, базы данных, GPU или DAVM (готовые виртуальные машины для аналитики).

В облачных вычислениях выделяют три основных модели предоставления услуг:

– IaaS (инфраструктура как сервис);

– PaaS (платформа как сервис);

– SaaS (программное обеспечение как сервис).

Использование облачных служб (Cloud Computing Services) и облачных ресурсов помогает избежать бизнесу капитальных затрат на собственную инфраструктуру и более быстро масштабироваться.

Облачные модели «программное обеспечение как сервис» (SaaS) и «данные как сервис» (DaaS) уже используют более 15 % крупных компаний. Эти хостируемые сервисы приобрели популярность, поскольку избавляют организацию от необходимости массовой установки и обслуживания программного обеспечения клиент/сервер, быстро развертываются, а данные постоянно пополняются и обновляются, остаются актуальными.

Некоторые хостинг-провайдеры предоставляют больше свободы при настройке облачных сервисов. Например, дают возможность устанавливать те или иные приложения на удаленных компьютерах и использовать их с любого стороннего устройства, включая мобильное.

Облачная сеть выстраивается из дата-центров. Это хранилище, в котором собирается и обрабатывается информация. Дата-центры могут быть территориально удалены друг от друга и связаны на большом расстоянии по сети. Их обслуживают хостинг-провайдеры. Пользователи подключаются к облачной инфраструктуре через Интернет, получая возможность работать со своими инструментами.

Облачные сервисы бывают разных видов. Условно можно выделить три категории:

1) *частные* – принадлежат компании и работают на ее оборудовании; такое решение стоит дорого, так как все затраты по обслуживанию и администрированию ложатся на бизнес;

2) *публичные* – содержатся облачным провайдером; компании платят за ресурсы, которые им нужны для работы;

3) *смешанные* – одна часть инструментов находится в публичном облаке, а другая часть – на частном. Такой подход хорошо зарекомендовал себя в том случае, если компании нужно хранить большой объем конфиденциальных данных на закрытом сервере в приватном облаке, но при этом она использует сторонние аналитические инструменты и приложения, которые можно запускать на публичных облачных платформах.

Облачные сервисы также помогают:

– автоматизировать бизнес-процессы с помощью CRM и других инструментов;

– наладить внутренние и внешние коммуникации: создать безопасный и быстрый мессенджер для общения между сотрудниками компании или собственную онлайн-платформу для взаимодействия с клиентами (интернет-телефония, чаты);

– настроить отчетность;

– ускорить учет: приложения из серии Metabase помогают собирать важные для компании данные из различных источников и представлять их в виде удобных схем и таблиц;

– защитить данные.

Облачные вычисления становятся одной из главных тенденций в развитии нефтегазового сектора. Они помогают сократить ресурсы на развертывание и поддержание локальных систем, а также делают управление данными более эффективным.

Какие возможности открывают облачные вычисления?

• Повышают эффективность работы и производства, предоставляя бесперебойный доступ к необходимым данным для анализа и принятия дальнейших решений.

• Избавляют от ограничений локальной памяти, поскольку позволяют хранить и обрабатывать данные на удаленных серверах.

• Делают цифровую трансформацию гибкой и доступной: оптимизируют процессы и обеспечивают плавный переход к новым технологиям.

• Упрощают развертывание ИТ-инфраструктуры. Зачастую требуется обеспечить ИТ-инфраструктуру во временных офисах, на этапах строительства объекта или в удаленных сложных локациях. При этом строить там собственные дата-центры или проводить работы по установке ИТ-оборудования, администрированию и отладке нецелесообразно, дорого и требует много времени. При этом облачная инфраструктура готова к работе практически сразу (рис. 3.5) и позволяет мобильно перемещать работу с одной площадки на другую без существенных затрат.

• Повышают безопасность и защищают конфиденциальные данные о добыче, транспортировке или переработке сырья от потенциальных внешних угроз.

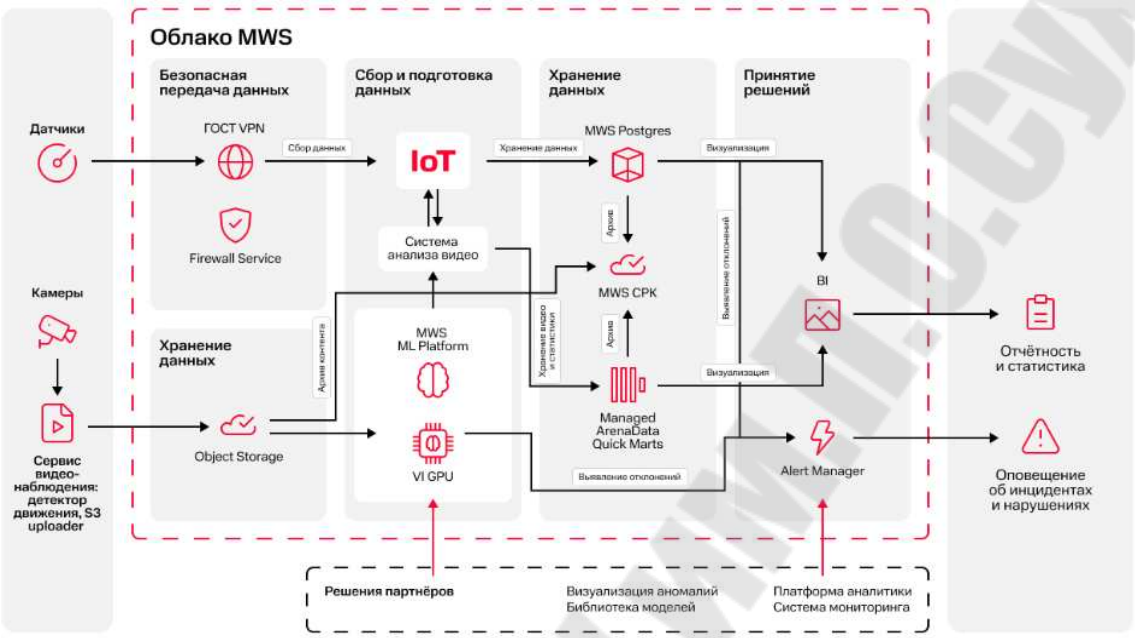

Рис. 3.5. Схема работы в облаке сервиса видеонаблюдения с детектором движения и камерами

Возможности в облаке

– 01 – контроль безопасности при добыче и переработке;

– виртуальные пропуски на объект/внутри объекта через опознавание лиц или биометрию;

– проверка наличия средств индивидуальной защиты (СИЗ) у сотрудников;

– контроль присутствия сотрудника на рабочем месте;

– контроль температуры оборудования;

– выявление движения объектов в зонах повышенного риска;

– оповещение о выявленных инцидентах;

– повышение безопасности труда;

– 02 – сокращение случаев несанкционированного доступа в помещения;

– 03 – сокращение числа поломок оборудования и других инцидентов по всей цепочке добычи, транспортировки и переработки;

– 04 – предотвращение аварийного состояния и других отклонений в работе ключевых установок;

– 05 – снижение капитальных и операционных затрат на разведку и эксплуатацию месторождений, а также ИТ-инфраструктуру;

– 06 – быстрое масштабирование вычислительных мощностей;

– 07 – повышение надежности и безопасности ИТ-инфраструктуры.

3.6. Промышленный Интернет вещей (IIoT)

Интернет вещей (IoT) – это система, которая объединяет устройства в компьютерную сеть и позволяет им собирать, анализировать, обрабатывать и передавать данные другим объектам через программное обеспечение, приложения или технические устройства (рис. 3.6).

IoT-устройства функционируют самостоятельно, хотя люди могут настраивать их или предоставлять доступ к данным. IoT-системы работают в режиме реального времени и обычно состоят из сети умных устройств и облачной платформы, к которой они подключены с помощью Wi-Fi, Bluetooth или других видов связи.

Объем мирового рынка Интернета вещей стремительно растет. Это связано с повсеместным внедрением ИИ и систем с машинным обучением. Росту рынка способствует также увеличение числа пользователей «умных» устройств, смартфонов и растущий спрос на энергосбережение.

Стандарт СТБ 2623-2023 «Интернет вещей. Термины и определения» устанавливает термины и определения основных понятий в области Интернета вещей.

Термины, установленные в настоящем стандарте, предназначены для применения всеми субъектами хозяйствования и органами управления в рамках исследования, разработки, производства и использования компонентов Интернета вещей, в научно-технической и справочной литературе.

Стандарт разработан с учетом основных нормативных положений международного стандарта ISO/IEC 20924:2018 «Информационные технологии. Интернет вещей (IoT). Словарь» (введен 01.06.2023).

Рис. 3.6. Сетевые технологии для Интернета вещей

Промышленная сеть Интернета вещей (IIoT) – это комплекс взаимосвязанных датчиков, контроллеров, устройств и программного обеспечения, используемых на промышленных предприятиях для автоматического сбора, передачи, анализа и использования данных о производственных процессах в реальном времени (рис. 3.6).

Основная цель IIoT – повышение эффективности, оптимизация работы оборудования, снижение затрат и управление производством без прямого участия человека, что способствует цифровой трансформации и Индустрии 4.0.

Промышленный Интернет вещей (ПИВ) – наиболее активно развивающееся направление в нефтегазовых компаниях. Представляет собой скоординированную сеть из физических устройств, датчиков с встроенными ИТ-инструментами для автоматического сбора и передачи данных с технологического оборудования с целью последующего анализа данных посредством различных программных продуктов и формирования рекомендаций, в том числе с помощью методов машинного обучения.

Архитектура ПИВ состоит из трех уровней.

Первый уровень является краевым и предполагает встраивание в систему системы интеллектуальных датчиков на различные виды оборудования, задача которых – улавливание изменения различных параметров и последующее их преобразование в цифровой вид. В частности, только на одной скважине может быть до 25 датчиков, передающих информацию об оборотах ротора, ходов насоса, температуры

пластовой жидкости в области перфорации продуктивного пласта и др.

В настоящее время активизировались НИОКР по разработке средств мониторинга следующего поколения, позволяющих получать и передавать в постоянном режиме информацию, для получения которой ранее требовалась остановка скважины с проведением исследований [15]. Создаются системы многофазного и виртуального измерения расхода [16, 17]. Система датчиков является базовой частью построения центрального диагностического мониторинга [18], что обусловливает критерии их отбора для внедрения, такие как точность и диапазон измерений, рабочая температура, время безотказной работы, размер и вес, защищенность корпуса, стабильность передачи данных.

Первый уровень основан на автоматизации добычного промысла, в ходе которого происходит оснащение скважин и технологического оборудования месторождения системами телеметрии [19] и визуального наблюдения [20], с целью передачи цифровых данных с месторождения в режиме реального времени, что требует масштабного развития интернет-инфраструктуры. Внедрение технологий интернет-связи 5G (~5 Гбит/с) на всей территории России является среднесрочной задачей, в то время как в Китае активно развивается Интернет с передачей данных со скоростью ~10 Гбит/с.

Второй уровень – это облачные серверы, собирающие и хранящие информацию с датчиков, объемы передачи которой достигают 2 Тб/час. Существуют проблемы непосредственно с серверным оборудованием, маршрутизаторами, компьютерами вследствие нарастающих санкций.

В настоящее время в нефтегазовой отрасли используются серверы отечественного производства – 6,3 %, коммутаторы – 10,2 %, системы хранения данных – 3,6 %, персональные компьютеры – 12,7 %. Следует отметить, что использование информационных и коммуникационных технологий присутствует не во всех организациях.

Третий уровень – это обработка программным обеспечением различных данных, хранящихся на сервере. Нефтегазовые компании более активны в данном направлении. Например, ПАО «НК «Роснефть» создала комплекс корпоративных программных продуктов, таких как «РН-ГЕОСИМ», «Горизонт+», «Сигма» GPT-системы, «РН-СЕЙСМ», «РНПЕТРОЛОГ» и др. [52]. Разрабатываются системы по оптимизации добычи с помощью интерпретации промысловой информации методами машинного обучения и ИИ [24–27]. 2022 год ознаменовал собой полномасштабное начало разработки программ циф-

ровой трансформации в нефтегазовых компаниях, включающее такие направления, как цифровое месторождение, собственная платформа цифрового интернета, цифровая цепочка поставок, цифровой завод и др.

От обычного промысла к интеллектуальному

В течение последних лет в нефтегазовой отрасли часто встречается понятие «умное месторождение», или «интеллектуальное месторождение», как термин, описывающий систему автоматического мониторинга и контроля физических процессов с последующей адаптацией интегральной модели в режиме реального времени [28].

Однако официально не определено, какие месторождения считать «умными». Большинство производств сейчас является во многом автоматизированным, однако ни одно не обходится без участия человека. Переход к интеллектуальному управлению промыслом, как показано на рис. 3.7, не только влечет за собой изменение управления технологическим процессом добычи и переработки углеводородов, но и вызывает трансформацию существующих бизнес-процессов нефтегазового предприятия в целом.

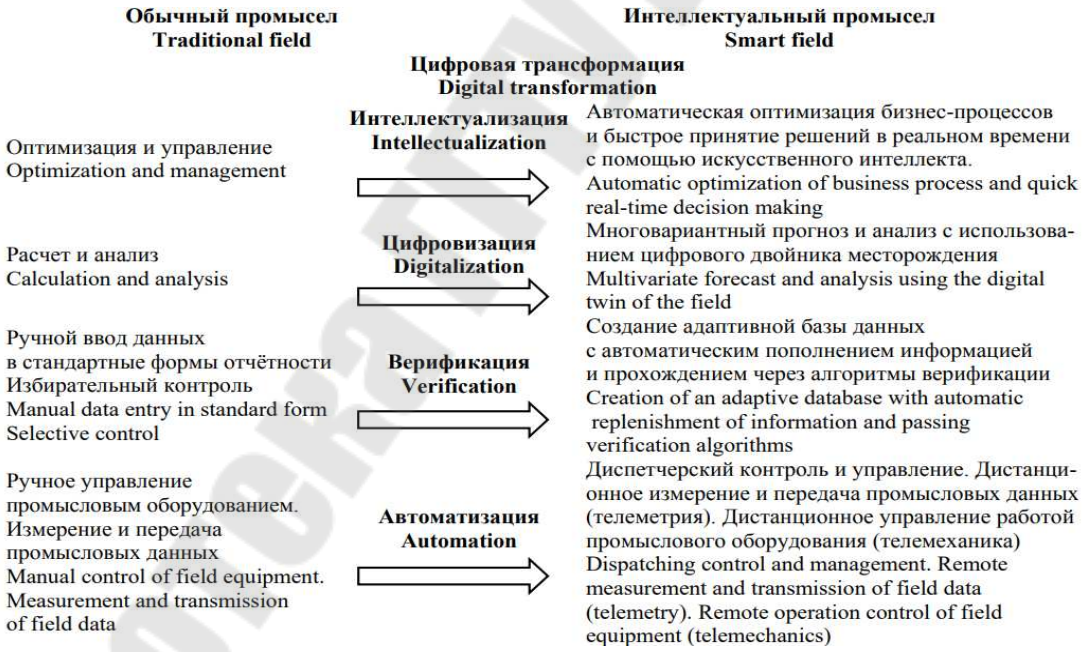

Рис. 3.7. Этапы трансформации при переходе к интеллектуальному промыслу (https://earchive.tpu.ru/bitstream/11683/123538/1/bulletin_tpu-2025-v336-i5-19.pdf)

Для интеллектуализации промысла необходимо его автоматизировать, что включает в себя дистанционный контроль и управление всеми объектами. Необходимо создать центр данных и обеспечить автоматическую оптимизацию процессов в реальном времени.

Переход от традиционных неавтоматизированных промыслов к современным интеллектуальным осуществляется в четыре этапа:

1. Автоматизированный промысел предполагает оснащение системами телеметрии и телемеханики, наличие диспетчерского контроля и оперативное управление (в том числе аварийная остановка) отдельными технологическими процессами и оборудованием по заданным алгоритмам.

2. Верифицированный промысел обозначает развитие систем баз данных, в результате чего информация с систем телеметрии автоматически подгружается. Дополнительно необходимо прохождение входящих данных через алгоритмы автоматической верификации на предмет ошибочных значений и зашумленных результатов для их исключения из общей выборки информации.

3. Цифровой промысел предполагает интеграцию оцифрованных данных с базой данных, что обеспечивает возможность анализа текущей ситуации на основе мониторинга постоянно поступающей информации, а также позволяет моделировать все технологические процессы и, следовательно, прогнозировать варианты сценариев за счет расчета параметров всей системы добычи и подготовки углеводородов, что в совокупности определяет цифровизацию. Управление промыслом реализуется с применением телемеханики на основе результатов расчетов и согласования оптимального технологического режима между промысловыми подразделениями.

4. Интеллектуальный промысел характеризуется наличием ИИ в самом широком смысле, задачей которого является автоматическая оптимизация как текущих, так и долгосрочных условий эксплуатации на основе многовариантных модельных расчетов, принимая во внимание заданные внешние параметры, такие как план добычи, экономические показатели, данные о персонале, оснащение и материально-технические ресурсы. Кроме того, он поддерживает автоматическое управление процессами в реальном времени.

Таким образом, основное отличие «интеллектуального» промысла от традиционного заключается в системе оперативного управления процессами добычи углеводородов, которая обеспечивает автоматическую оптимизацию производства за счет своевременного выявления возникающих проблем и принятия оптимальных решений в режиме реального времени.

Центральным элементом интеллектуальной системы управления разработкой месторождений углеводородов выступает программно-

аппаратный комплекс [29]. Он гарантирует непрерывную работу ЦДМ для анализа всей необходимой промысловой информации, которая поступает в режиме реального времени посредством автоматизированных систем производства.

В результате осуществляется:

– оперативное выявление любых отклонений от проектных параметров;

– определение эффективных управленческих решений на основе многовариантных прогнозных расчетов;

– самостоятельная реализация решений с помощью систем телемеханики (на первых этапах – с разрешения оператора, затем – под контролем оператора).

Управленческий аспект создания интеллектуального промысла необходимо рассматривать с позиций совмещения функциональных обязанностей работников предприятия, ИИ и других цифровых технологий.

Оптимальной является трехуровневая система:

– на уровне компании;

– добывающего предприятия (дочернего подразделения);

– добычного промысла.

Цифровая трансформация актуализирует формирование центров на разных уровнях, объединяющих специалистов из разных сфер и ИИ. На базе ИИ могут быть созданы цифровой куратор для управления системой каждого уровня и цифровой помощник каждого работника, которые совершенствуются посредством машинного обучения с учетом меняющейся ситуация и появления разного рода задач.

В процессе реализации пилотных проектов планируется получение опыта оптимизации добычи и интеллектуального управления промыслами в различных условиях. В рамках проекта планировалось:

– создание на установке комплексной подготовки газа (УКПГ) высокопроизводительной САУП и организация ее взаимодействия со SCADA (Supervisory Control And Data Acquisition/Диспетчерское управление и сбор данных);

– установка на скважинах САР, обеспечивающих поддержание режимов работы скважин, заданных САУП, в том числе при сбоях в системах связи с УКПГ;

– применение высокоскоростного интегрированного моделирования и многоуровневой оптимизации;

– использование новых датчиков (дистанционный контроль обводнения скважин, сигнализатор эрозии и др.);

– применение технологий автоматической адаптации моделей и валидации поступающих данных;

– использование модуля экономического анализа в составе оптимизатора;

– формирование модульной концепции, позволяющей постепенно вовлекать в оптимизационный вычислительный цикл дополнительные производственные модули.

Ожидаемые ключевые эффекты следующие: а) прирост добычи газа по промыслу на ~3,2 % и конденсата на ~3 %; б) снижение расхода метанола на ~5 %.

В рамках крупных месторождений подобный результат может принести значимый экономический эффект. В настоящее время можно отметить, что работы в данном направлении ведут многие нефтегазодобывающие предприятия, совмещая параллельно разработки в области управления предприятием и системного инжиниринга с интеллектуализацией промысла [30].

Впоследствии системы могут оперативно дорабатываться, обеспечивая тем самым ускоренный переход к итоговому интеллектуальному предприятию.

Также цифровая трансформация активно внедряется в проектные организации, осуществляющие разработку технической документации, в начальные сегменты – ГРР, мониторинг и проектирование разработки, сопровождение бурения и создание проектной документации по обустройству месторождений [33].

Во многих направлениях большое внимание уделяется принципам формирования баз данных и верификации входящей информации. Именно в рамках проектной деятельности на этапе работы с промысловой информацией обнаруживаются нефизичные и малодостоверные данные наблюдений или результаты исследований, что требует развития направления разработки механизмов работы с базой на основе стохастических моделей, методов машинного обучения или нейронных сетей с целью контроля входящей в базу информации.

Цифровая трансформация в широком смысле ориентирована на достижение стратегической задачи – сохранение конкурентоспособности в условиях усиливающихся по масштабам воздействия вызовов, является изменением существующей бизнес-модели, ориентированной на определенные рынки сбыта, продуктовые корзины, логистические карты, макроэкономические параметры и институциональное окружение. Аналогично может рассматриваться интеллектуализация:

В узком смысле как цифровой инструмент для помощи в решении конкретных задач, в широком смысле как управленческая система, наделенная правами принятия и реализации решений. Ученые А. В. Карсаков, П. Н. Зятиков, И. В. Шарф выделяют три основных блока, внутри которых происходит цифровая трансформация (рис. 3.8).

Рис. 3.8. Структура цифровой трансформации нефтегазовой отрасли

Протекающие внутриблоковые процессы являются одновременно параллельными и взаимозависимыми: внедрение и совершенствование самостоятельных технологий в одном блоке дает толчок к развитию в других, которые, в свою очередь, открывают возможности к развитию качественно новых систем в целом по отрасли.

Типовая схема реализации цифровых проектов в нефтегазовой сфере отображена на рис. 3.9 в определенной последовательности.

Текущие объемы промысловой информации требуют регулярного обновления архитектуры базы данных и ее автоматической экспресс-верификации.

Таким образом, *цифровая трансформация нефтегазовой отрасли* – это преобразование системы управления нефтегазовой компании и ее дочерних подразделений на основе цифровизации и интеллектуализации для оптимизации технологических процессов с целью сохранения конкурентоспособности компании в быстроменяющихся макроэкономических, макроэнергетических и институциональных условиях на мировом рынке углеводородов.

Рис. 3.9. Типовая схема реализации цифровых проектов в нефтегазовой сфере

Интеллектуализация нефтегазовой отрасли – трансформация в управлении нефтегазовой компанией, ее дочерними подразделениями и производственными участками на основе автоматизации и цифровизации всех процессов (производственных, технологических и управленческих) с целью их оптимизации, что позволит снизить операционные и капитальные издержки и улучшить производственно-экономические показатели, что в конечном итоге трансформирует всю бизнес-модель управления (рис. 3.10).

Для запуска промышленной сети Интернета вещей (Интернета предметов) необходимо выполнить следующие шаги:

• **Планирование и стратегия:** определить цели и задачи внедрения промышленного Интернета вещей. Разработать стратегию, которая включает выбор технологий, определение области применения и оптимальную инфраструктуру.

• **Выбор оборудования и датчиков:** исследовать и выбрать подходящие датчики и оборудование, способные собирать данные в реальном времени. Они должны обладать высоким качеством, надежностью и совместимостью с оборудованием и выбранными технологиями.

• **Соединение и сетевая инфраструктура:** должна обеспечивать передачу данных от датчиков к центральной системе управления с использованием вариантов связи, таких как беспроводные технологии (например, Wi-Fi, Bluetooth, LoRaWAN) или проводные сети.

• **Разработка программного обеспечения:** для управления и обработки данных, собранных от датчиков, которая позволит мониторить данные 24/7, анализировать их и предпринимать соответствующие действия.

• **Интеграция и тестирование** оборудования, датчиков и программного обеспечения в единую систему с проверкой функциональности и производительности для подтверждения корректной работы и соответствия требованиям.

• **Внедрение и масштабирование** промышленного Интернета вещей в реальной среде с оценкой результатов и производительности системы для последующего внесения необходимых корректировок и расширения ее в случае необходимости.

• **Обеспечение безопасности** данных и защита их от возможных угроз путем шифрования данных, аутентификации и контроля доступа.

• **Поддержка и обслуживание** системы, включая мониторинг работоспособности, обновление программного обеспечения и оборудования.

При переходе на IIOT производственные системы управления работают так: крупная распределительная система управления (РСУ) представляет собой сложную сеть датчиков, исполнительных механизмов, контроллеров и вычислительных ресурсов.

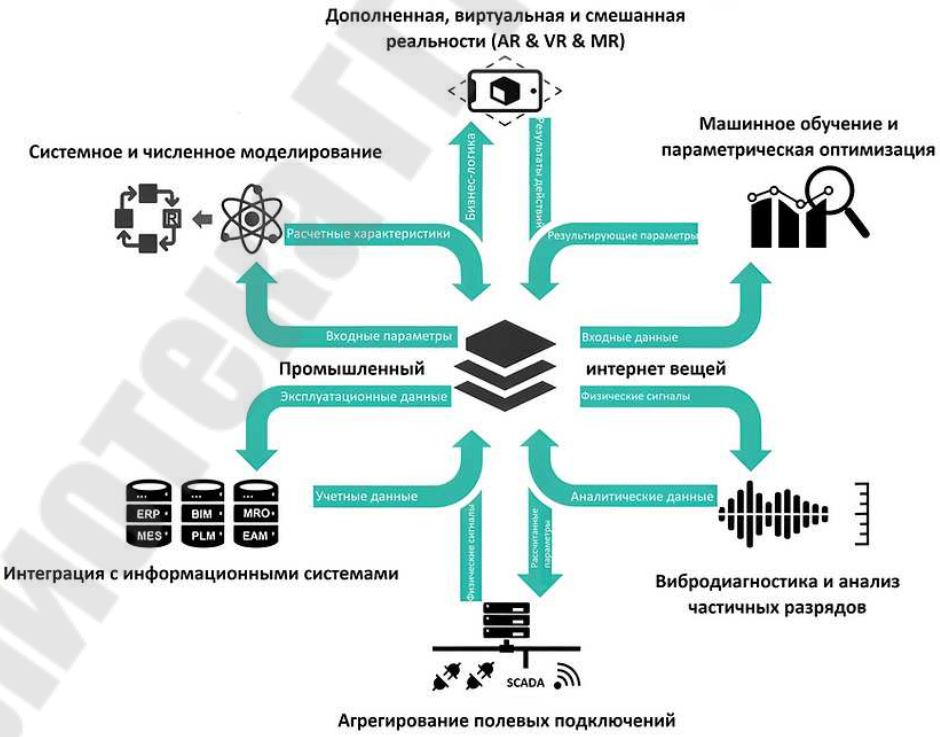

Рис. 3.10. Схема внедрения промышленного Интернета вещей при интеллектуализации нефтегазовой отрасли

Нижние уровни РСУ, как правило, являются автономными и отвечают за управление технологическими процессами в реальном времени, работая с высокой степенью безопасности и надежности.

На более высоких уровнях реализуются различные надзорные функции, включая упреждающее и диспетчерское управление, человеко-машинные интерфейсы, обеспечивающие участие в управлении операторов.

На самом верхнем уровне располагаются средства непрерывного сбора и анализа данных о процессах, а также инструменты планирования и составления графиков производственной деятельности, которые передаются на нижние уровни для исполнения. Общая архитектура приведена на рис. 3.11.

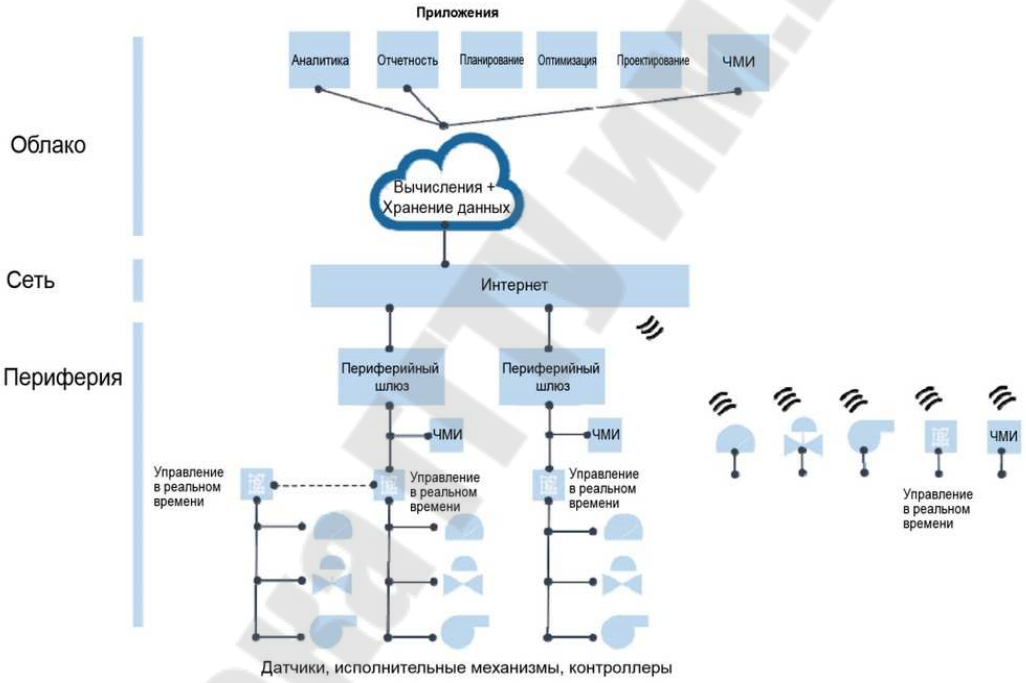

Рис. 3.11. Общая архитектура IIOT производственной системы (https://www.cnews.ru/reviews/bi_bigdata_2016/articles/promyshlennyj_internet_veshchej_kak_ne_slomat_to_chto_rabotaet)

IIOT объединяет широкий спектр промышленных устройств, включая датчики, исполнительные механизмы и контроллеры. Находясь в непосредственной близости от производственного процесса, эти устройства постоянно взаимодействуют с облачными сервисами. Кроме того, промышленные устройства могут действовать совместно, выполняя определенный набор функций. Например, совокупность датчиков, исполнительных механизмов, контроллеров и человеко-

машинных интерфейсов может обеспечить оперативный контроль и управление технологической установкой или зоной.

В целом переход к архитектуре IIOT позволит создать систему, лишенную ограничений иерархической структуры РСУ.

В целом IIOT представляет собой более сложную и специализированную разновидность Интернета вещей, разработанную для удовлетворения потребностей промышленного сектора, который помогает автоматизировать и оптимизировать производственные процессы, повышать производительность, снижать затраты, улучшать безопасность и обеспечивать более высокое качество продукции. Эти особенности делают промышленный Интернет вещей ключевым инструментом цифровой трансформации в промышленности.

IIOT состоит из следующих компонентов:

– *устройства сбора данных* (*sensors*) – устройства, которые собирают данные о состоянии оборудования, температуре, влажности и других параметрах производства;

– *система передачи данных* (*communication system*) – система, которая передает данные от устройств сбора данных к центральному серверу;

– *центральный сервер* (*central server*) – сервер, который принимает данные от устройств сбора данных и обрабатывает их;

– *программное обеспечение для анализа данных* (*data analytics software*) – программа, которая обрабатывает и анализирует данные, полученные от устройств сбора данных;

– *программное обеспечение для управления данными* (*data management software*) – программа, которая управляет данными, полученными от устройств сбора данных.

Преимущества промышленного Интернета вещей (плюсы):

– *улучшение эффективности производства* – промышленный Интернет вещей позволяет оптимизировать производственные процессы и уменьшить количество отходов;

– *увеличение безопасности производства* – промышленный интернет вещей позволяет быстро обнаруживать потенциальные проблемы и предотвращать аварии;

– *оптимизация затрат на обслуживание оборудования* – промышленный Интернет вещей позволяет своевременно обнаруживать неисправности и проводить профилактику, что снижает расходы на ремонт и замену оборудования;

– *улучшение качества продукции* – благодаря сбору и анализу данных о производственных процессах, промышленный Интернет ве-

щей позволяет выявлять проблемы в производственной линии и принимать меры для их устранения, что улучшает качество продукции;

– *оптимизация логистики* – промышленный Интернет вещей позволяет отслеживать перемещение грузов и оптимизировать логистические процессы, что уменьшает затраты на транспортировку и ускоряет доставку;

– *улучшение управления ресурсами* – промышленный Интернет вещей позволяет контролировать расход энергии, воды и других ресурсов, что позволяет сократить расходы на их использование.

Рассмотрим вызовы и проблемы при внедрении промышленного Интернета вещей (минусы):

– *большие затраты на внедрение* – внедрение промышленного Интернета вещей может быть дорогим процессом, требующим инвестиций в новое оборудование и программное обеспечение;

– *необходимость обучения персонала* – для эффективного использования промышленного Интернета вещей необходимо обучить персонал, что может занять значительное время и стоить дополнительных затрат;

– *проблемы с конфиденциальностью данных* – сбор и передача большого количества данных может привести к проблемам с конфиденциальностью и безопасностью данных;

– *необходимость совместимости с существующим оборудованием* – для внедрения промышленного Интернета вещей необходимо убедиться, что новое оборудование совместимо с уже существующим.

В то же время внедрение IIOT помогает повышать производительность и снижать затраты на производстве следующим образом:

– позволяет автоматизировать множество производственных процессов, уменьшая зависимость от человеческого фактора и сокращая время на выполнение задач;

– IIOT-устройства собирают и передают информацию о работе оборудования и производственных линий в реальном времени, что позволяет оперативно выявлять проблемы, принимать решения и оптимизировать процессы;

– IIOT дает возможность анализировать данные с датчиков и машин для прогнозирования потенциальных отказов и проведения планового обслуживания (предиктивное обслуживание), что снижает простои оборудования и затраты на ремонт;

– используя данные от IIOT-устройств, предприятия могут контролировать и оптимизировать энергопотребление, снижая энергетические затраты и уменьшая воздействие на окружающую среду;

– IIOT обеспечивает точное отслеживание материалов, компонентов и готовой продукции, что упрощает управление запасами, сокращает издержки на хранение и улучшает логистику;

– IIOT-устройства могут непрерывно контролировать качество продукции на разных этапах производства, обеспечивая высокий уровень качества и снижение отклонений и дефектов;

– IIOT позволяет мониторить состояние оборудования и опасные факторы производственной среды, что помогает предотвратить инциденты и обеспечивает безопасность сотрудников;

– IIOT обеспечивает сбор данных о работе сотрудников, что позволяет анализировать их производительность, определить зоны ответственности и проводить более эффективное распределение рабочей нагрузки. Это помогает повысить производительность и снизить издержки на оплату труда;

– IIOT способствует более глубокой интеграции различных систем и обмену данными между ними, что упрощает управление производственными процессами и сокращает время на обработку информации;

– IIOT позволяет создавать цифровые двойники физических объектов и систем для проведения виртуального моделирования и оптимизации процессов без риска для реального оборудования;

– IIOT обеспечивает быстрый доступ к данным и аналитике, что способствует инновационному развитию и позволяет предприятиям быстро адаптироваться к изменяющимся рыночным условиям и потребностям заказчиков.

Пример внедрения промышленного Интернета вещей

• *Мониторинг и контроль оборудования*: установка датчиков на машины для отслеживания рабочих параметров и определения необходимости технического обслуживания.

• *Автоматизированные производственные линии*: применение роботов и автоматизированных систем для увеличения производительности и качества продукции.

• *Управление инвентарем*: использование IoT-устройств для отслеживания количества сырья, полуфабрикатов и готовой продукции на складе.

• *Системы контроля качества*: применение IoT-технологий для автоматической проверки качества продукции на всех этапах производства.

• *Умная сеть энергоснабжения*: оптимизация потребления электроэнергии на предприятии с помощью IoT-устройств и алгоритмов анализа данных.

• *Управление энергоэффективностью*: мониторинг и оптимизация потребления энергоресурсов на заводе с использованием IoT-технологий.

• *Умные системы безопасности*: интеграция систем видеонаблюдения, контроля доступа и датчиков безопасности для обеспечения надежной защиты предприятия.

• *Прогнозирование и предотвращение аварий*: анализ данных с датчиков для своевременного выявления и устранения потенциальных проблем на производстве.

• *Автоматизация транспортных процессов*: применение беспилотных транспортных средств и систем управления для ускорения и оптимизации внутризаводской логистики.

• *Цифровые двойники*: создание виртуальных моделей оборудования и процессов для анализа и оптимизации производства.

• *Управление техническим обслуживанием*: автоматизация процесса планирования и выполнения регламентных работ на основе данных с IoT-устройств.

• *Умное управление отходами*: мониторинг и оптимизация системы обращения с отходами на предприятии с использованием IoT-технологий.

• *Умные системы вентиляции и кондиционирования*: автоматическое регулирование параметров вентиляции и кондиционирования на основе данных с датчиков.

• *Управление водоснабжением и канализацией*: мониторинг и контроль систем водоснабжения и канализации на предприятии с использованием IoT-технологий.

• *Управление химическими процессами*: применение IoT-устройств для контроля и оптимизации химических реакций в процессе производства.

• *Дистанционный мониторинг и управление оборудованием*: удаленное управление и контроль работы машин и аппаратов через Интернет с использованием IoT-технологий.

• *Системы автоматической идентификации*: использование RFID-меток и считывателей для отслеживания перемещения товаров и материалов на предприятии.

• *Автоматизированные системы пожарной безопасности*: применение IoT-датчиков для мониторинга температуры, дыма и пламени с целью своевременного обнаружения пожаров.

• *Беспилотные летательные аппараты для мониторинга*: использование дронов для контроля и инспекции оборудования и объектов на предприятии.

• *Управление производственными процессами*: автоматизация и оптимизация рабочих процессов на основе данных, полученных от IoT-устройств.

• *Системы управления персоналом*: использование IoT-технологий для мониторинга и анализа работы сотрудников, определения зон ответственности и повышения эффективности труда.

• *Управление агрегатами на шахтах*: мониторинг и контроль работы добычного оборудования на шахтах с использованием IoT-устройств.

• *Умная сварка*: применение IoT-технологий для контроля и оптимизации процессов сварки на производстве.

• *Управление транспортными средствами на территории завода*: использование IoT-устройств для контроля и оптимизации работы автомобилей, спецтехники и погрузчиков.

• *Мониторинг состояния окружающей среды*: использование IoT-датчиков для контроля уровня загрязнения воздуха, воды и почвы на территории предприятия.

• *Системы автоматического контроля температуры и влажности*: использование IoT-датчиков для поддержания оптимальных условий в производственных цехах и складских помещениях.

• *Управление электропитанием и автоматизированные электрощиты*: применение IoT-устройств для мониторинга и контроля распределения электроэнергии на предприятии.

• *Мониторинг и контроль системы отопления*: использование IoT-технологий для автоматического регулирования температуры отопления в зависимости от погодных условий и потребностей производства.

• *Управление процессами сборки и упаковки*: интеграция IoT-технологий в системы сборки и упаковки продукции для оптимизации рабочих процессов и снижения затрат на труд.

Эти примеры демонстрируют возможности промышленного Интернета вещей для оптимизации и автоматизации производственных процессов на предприятиях и заводах. Применение IoT-технологий позволяет повышать эффективность работы, снижать затраты и улучшать качество продукции.

При практическом внедрении цифровых технологий крупными нефтяными компаниями они дают свои названия специальных проектов, которые можно отнести к категории «умное/интеллектуальное» производство [31]:

1) «умные» скважины – Smart Wells (Schlumberger);

2) «умные» операции – Smart Operations (Petoro);

3)) «интегрированные» операции – Integrated Operations (Statoil, OLF);

4) «электронное» управление – eOperations (North Hydro);

5) «управление в режиме реального времени» – Real Time Operations (Halliburton);

6) «правильное» направление – eDrift (OD);

7) «интегрированная модель управления активами» – Integrated Asset Operation Model (IAOM), ADCO;

8) «умное» месторождение – Smart Field (Shell);

9) «интеллектуальное» месторождение – i-field (Chevron);

10) «месторождение будущего» – Field of the future (BP);

11) «цифровое» нефтяное месторождение будущего – Digital oil field of the future DOFF (CERA);

12) оптимизация «интеллектуального» месторождения и удаленное управление – Intelligent Field Optimisation and Remote Management/INFORM (Cap Gemini) и др.

Все эти системы довольно сходны между собой по своим основным целям и локальным задачам: они призваны с высокой степенью достоверности моделировать различные сценарии развития ситуации на нефтегазовом производстве и предоставлять возможность выбора наиболее оптимальных решений (в том числе и по более эффективному использованию высококвалифицированных специалистов компании). Кроме того, существуют различные варианты названий данного подхода (как на русском, так и на английском языке).

Все эти технологии обеспечивают «интеллектуализацию» процесса добычи, транспортировки и переработки нефти. Поэтому при рассмотрении таких инновационных технологий необходимо учитывать, что в переводе с латинского «интеллект» означает «познание, понимание или рассудок». Присутствие интеллекта в любой сложной системе, будь она биологическая (человек) или даже инженерная (скважина, нефтепромысел, нефтепроводы и т. д.), предполагает возможность и наличие самостоятельного регулирования и оптимизации множественных внутренних параметров ее работы по отношению к

разнообразным и постоянно изменяющимся условиям или проявлениям воздействий внешней среды.

3.7. Инженерные симуляторы

Инженерные симуляторы в нефтегазовой отрасли – это программные комплексы для динамического моделирования процессов добычи и транспортировки углеводородов, которые позволяют повысить эффективность работы оборудования, снизить затраты и риски, а также тренировать персонал. Такие программы анализируют данные с месторождений, оптимизируют подбор и работу оборудования, прогнозируют ресурсные показатели и помогают справляться с осложнениями в добыче.

Например, симулятор бурения скважин – специализированный программный комплекс программного модуля добычи нефти и газа, позволяющий при помощи интерактивного взаимодействия с трехмерной моделью исследовать технологический процесс бурения нефтяных скважин, а также отрабатывать навыки управления буровым оборудованием (рис. 3.12). Реализована имитация процесса бурения в процессе проводки скважины с возможностью изменения режима бурения, отработки технологических ошибок и ликвидации нештатных ситуаций при бурении. Реализована проверка и оценка имитационного сценария.

Рис. 3.12. Общий вид комплекса симулятора бурения скважин

Основные функции инженерных симуляторов:

– *динамическое моделирование*: симуляторы позволяют в реальном времени моделировать весь технологический процесс бурения, добычи и транспортировки нефти и газа;

– *оптимизация работы оборудования*: на основе данных о скважине и месторождении симуляторы могут рекомендовать оптимальное оборудование (например, насосы) и его рабочие параметры для повышения добычи;

– *прогнозирование и предотвращение проблем*: симуляторы способны предсказывать возможные осложнения в процессе добычи и указывать на меры по их устранению;

– *управление рисками*: симуляторы помогают снизить риски простоев, которые могут привести к финансовым потерям и экологическим последствиям;

– *тренажер для специалистов*: программное обеспечение может использоваться для обучения студентов и молодых специалистов, что повышает их квалификацию и способствует появлению нового поколения профессионалов в отрасли.

Внедрение инженерных симуляторов в научных специализированных центрах позволяет получать детальную информацию о процессе добычи, что необходимо для принятия обоснованных управленческих решений, помогает выбрать оптимальное насосное и поверхностное оборудование, а также настроить его работу в соответствии с условиями месторождения. Симуляторы дают возможность моделировать различные сценарии добычи и выбирать наиболее эффективные.

VR-тренажеры и AR-технологии становятся стандартами в нефтяной промышленности для обучения персонала действиям в аварийных ситуациях за счет безопасной имитации реальных сценариев. VR позволяет полностью погрузиться в виртуальную среду, а AR накладывает цифровую информацию на реальный мир, обеспечивая эффективное и реалистичное обучение без риска для жизни и здоровья.

Преимущества VR- и AR-технологий состоят в следующем:

– *безопасность*: сотрудники отрабатывают действия в критических ситуациях, не подвергая себя опасности и не нанося вреда оборудованию;

– *эффективность*: иммерсивное погружение и интерактивное обучение повышают запоминаемость, позволяя получать как теоретические, так и практические навыки;

– *гибкость*: тренировки можно проводить в то или иное удобное время и в любом месте, даже удаленно;

– *снижение затрат*: уменьшаются расходы на проведение реальных учений, а также на ремонт оборудования, который может потребоваться при ликвидации аварий;

– *игровой формат*: обучение в формате игры делает процесс более увлекательным и мотивирующим, особенно для молодого персонала.

Приведем примеры использования инженерных симуляторов:

– *VR-тренажеры*: используются для моделирования сложных и опасных сценариев, таких как пожары на установках или утечки нефти, где сотрудники должны отработать правильную последовательность действий;

– *AR-технологии*: могут использоваться для обучения в реальной рабочей среде. Например, через AR-очки сотрудник может видеть инструкции по проведению технического обслуживания или аварийного ремонта, наложенные на реальное оборудование;

– *комбинированное использование*: возможно создание гибридных сценариев, когда, например, специалист в реальном мире (с помощью AR-очков) взаимодействует с виртуальным объектом, созданным с помощью VR-технологий.

VR- и AR-системы постоянно развиваются, предлагая более реалистичную визуализацию и обратную связь (например, тактильную или силовую), что делает обучение еще более эффективным. Прогресс в области программного обеспечения и оборудования позволяет создавать все более сложные и реалистичные симуляции.

3.8. Блокчейн в нефтегазовой отрасли

Блокчейн (*blockchain*) – информационная технология, проводящая без посредников операции между равноправными участниками единой сети, такие как передача данных, перевод средств, заключение контракта и т. д. [1]. Уникальность данной технологии заключается в прозрачности и открытости информации, установлении подлинности данных, защите от искажения информации или ее уничтожения. Международные нефтегазовые компании постепенно начинают свои разработки с ввода технологии блокчейн в виде торговой площадки для выполнения сделок с нефтью на спот-рынке. Применяемая технология блокчейн дает возможность наблюдения за операциями купли-

продажи. При этом идет огромный учет данных для обеспечения безопасности транзакций и предоставления права всем заинтересованным сторонам держать под контролем процесс каждой сделки.

Но современные ученые до сих пор не пришли к единому мнению о том, является ли блокчейн новой технологией управления или базой хранения информации. На данный момент можно отметить, что блокчейн находится в состоянии перехода от обычной базы данных к новой управленческой технологии, которая позволяет сократить затраты, оптимизировать различные бизнес-процессы, сократить время на осуществление определенных операций, что в конечном итоге повышает конкурентоспособность предприятия. Технология blockchain сегодня вполне соответствует общему тренду: мир становится все более и более цифровым, поэтому это просто еще одно течение, которое будет способствовать глобальной digital-эволюции.

3.9. Операционная эффективность предприятия за счет цифровых инструментов SCADA, MES, ERP

SCADA-системы (Supervisory Control And Data Acquisition – диспетчерское управление и сбор данных) – это программно-аппаратные комплексы, предназначенные для сбора, обработки и отображения данных в реальном времени с промышленных объектов, позволяющие операторам осуществлять дистанционный контроль и управление технологическими процессами. Они включают в себя аппаратные средства (датчики, ПЛК), программное обеспечение для визуализации данных (HMI) и управления, а также коммуникационные протоколы для обмена информацией. SCADA-системы применяются в таких отраслях, как энергетика, производство, водоочистка для автоматизации и оптимизации их работы.

Системы оперативного управления производствами и предприятиями (или MES-системы) – это специализированное программное обеспечение, которое в реальном времени координирует, отслеживает, оптимизирует и документирует производственные процессы на всех этапах – от заказа сырья до выпуска готовой продукции. Их главная цель – синхронизация работы цехов и участков, эффективное использование ресурсов и сокращение длительности производственного цикла для повышения прибыли предприятия.

ERP-системы (Enterprise Resource Planning – планирование ресурсов предприятия) – это комплексные информационные системы,

которые интегрируют и автоматизируют такие основные бизнес-процессы в компании, как финансы, логистика, управление персоналом, производство и продажи, в единую платформу с общей базой данных. Основная цель – повысить эффективность, оптимизировать затраты и улучшить контроль над всеми аспектами бизнеса, предоставляя руководству актуальную и полную картину для принятия обоснованных решений.

Существуют как российские (например, на базе 1С), так и международные MES-решения, такие как Siemens Opcenter, SAP ME, AutoSuite и другие SCADA-пакеты, выполняющие множество функций, которые можно разделить на несколько групп:

– настройка SCADA на конкретную задачу (т. е. разработка программной части системы автоматизации);

– диспетчерское управление;

– автоматическое управление;

– хранение истории процессов;

– выполнение функций безопасности;

– выполнение общесистемных функций.

Одной из основных функций SCADA является разработка человеко-машинного интерфейса, т. е. SCADA одновременно является и человеко-машинным интерфейсом, и инструментом для его создания. Быстрота разработки существенно влияет на рентабельность фирмы, выполняющей работу по внедрению системы автоматизации, поэтому скорость разработки является основным показателем качества SCADA с точки зрения системного интегратора. В процесс разработки входят следующие операции:

– создание графического интерфейса (мнемосхем, графиков, таблиц, всплывающих окон, элементов для ввода команд оператора и т. д.);

– программирование и отладка алгоритмов работы системы автоматизации. Многие SCADA позволяют выполнять отладку системы как в режиме эмуляции оборудования, так и с подключенным оборудованием;

– настройка системы коммуникации (сетей, модемов, коммуникационных контроллеров и т. п.);

– создание баз данных и подключение к ним SCADA.

Как система диспетчерского управления SCADA может выполнять следующие задачи:

– взаимодействие с оператором (выдача визуальной и слуховой информации, передача в систему команд оператора);

– помощь оператору в принятии решений (функции экспертной системы);

– автоматическая сигнализация об авариях и критических ситуациях;

– выдача информационных сообщений на пульт оператора;

– ведение журнала событий в системе;

– извлечение информации из архива и представление ее оператору в удобном для восприятия виде;

– подготовка отчетов (например, распечатка таблицы температур, графиков смены операторов, перечня действий оператора);

– учет наработки технологического оборудования.

Основная часть задач автоматического управления выполняется, как правило, с помощью программируемого логического контроллера, однако часть задач может возлагаться на SCADA. Кроме того, в небольших системах управления программируемые логические контроллеры могут вообще отсутствовать, и тогда компьютер с установленной SCADA является единственным средством управления. SCADA обычно выполняет следующие задачи автоматического управления:

– автоматическое регулирование;

– управление последовательностью операций в системе автоматизации;

– адаптация к изменению условий протекания технологического процесса;

– автоматическая блокировка исполнительных устройств при выполнении заранее заданных условий.

Знание предыстории управляемого процесса позволяет улучшить будущее поведение системы, проанализировать причины возникновения опасных ситуаций или брака продукции, выявить ошибки оператора. Для создания истории система выполняет следующие операции:

– сбор данных и их обработка (цифровая фильтрация, интерполяция, сжатие, нормализация, масштабирование и т. д.);

– архивирование данных (действий оператора, собранных и обработанных данных, событий, алармов, графиков, экранных форм, файлов конфигурации, отчетов и т. п.);

– управление базами данных (реального времени и архивных).

Применение SCADA в системах удаленного доступа через Интернет резко повысило уязвимость SCADA. С одной стороны, существуют мощные управляющие подсистемы, которые обеспечивают оператору полный контроль над производственными процессами, в

том числе в стратегических секторах экономики, где любые сбои опасны, а с другой стороны, оператором может стать постороннее лицо. Таким образом, для защиты информационных комплексов, содержащих SCADA-системы, требуется соблюдение общих требований информационной безопасности.

Пренебрежение этой проблемой может приводить, например, к отказу в работе сетей электроснабжения, жизнеобеспечения, связи, отказу морских маяков, дорожных светофоров, к заражению воды неочищенными стоками и т. п. Возможны и более тяжелые последствия с человеческими жертвами или большим экономическим ущербом. Для повышения безопасности SCADA используют следующие методы:

– разграничение доступа к системе между разными категориями пользователей (у сменного оператора, технолога, программиста и директора должны быть разные права доступа к информации и к модификации настроек системы);

– защиту информации (путем шифрования информации и обеспечения секретности протоколов связи);

– обеспечение безопасности оператора благодаря его отдалению от опасного управляемого процесса (дистанционное управление). Дистанционный контроль и дистанционное управление являются типовыми требованиями Ростехнадзора и выполняются по проводной сети, радиоканалу (через GSM- или радиомодем), через Интернет и т. д.;

– специальные методы защиты от кибератак;

– применение межсетевых экранов.

Поскольку SCADA обычно является единственной программой для управления системой автоматизации, на нее могут возлагаться также некоторые общесистемные функции:

– осуществление взаимодействий между несколькими SCADA, между SCADA и другими программами (MS Office, базой данных, MATLAB и т. п.);

– диагностика аппаратуры, каналов связи и программного обеспечения.

В силу тех требований, которые предъявляются к системам SCADA, весь описанный выше спектр их функциональных возможностей определен и реализован практически во всех пакетах. Различаются SCADA-системы в основном только техническими особенностями реализации.

Несмотря на множество функций, выполняемых SCADA, основным ее отличительным признаком является наличие интерфейса

с пользователем. При отсутствии такого интерфейса перечисленные выше функции совпадают с функциями средств программирования контроллеров, а управление является автоматическим, без непосредственного участия человека (в отличие от диспетчерского).

Качество решений, принятых оператором (диспетчером), часто влияет не только на качество производимой продукции, но и на жизнь людей. Поэтому комфорт рабочего места, понятность интерфейса, наличие подсказок и блокировка явных ошибок оператора являются наиболее важными свойствами SCADA, а дальнейшее их развитие осуществляется в направлении улучшения эргономики и создания экспертных подсистем.

Международная ассоциация производителей систем управления производством MESA (Manufacturing Enterprise Solution Association) определила 11 основных функций MES-систем:

1) RAS (англ. *Resource Allocation and Status*) – контроль состояния и распределение ресурсов. Управление ресурсами: технологическим оборудованием, материалами, персоналом, обучением персонала, а также другими объектами, такими как документы, которые должны быть в наличии для начала производственной деятельности.

Обеспечивает детальную историю ресурсов и гарантирует, что оборудование соответствующим образом подготовлено для работы. Контролирует состояние ресурсов в реальном времени. Управление ресурсами включает резервирование и диспетчеризацию с целью достижения целей оперативного планирования;

2) ODS (англ. *Operations/Detail Scheduling*) – оперативное детальное планирование. Обеспечивает упорядочение производственных заданий, основанное на очередности, атрибутах, характеристиках и рецептах, связанных со спецификой изделий, таких как форма, цвет, последовательность операций и других, а также технологией производства. Цель – составить производственное расписание с минимальными перенастройками оборудования и параллельной работой производственных мощностей для уменьшения времени получения готового продукта и времени простоя;

3) DPU (англ. *Dispatching Production Units*) – диспетчеризация производства. Управляет потоком единиц продукции в виде заданий, заказов, серий, партий и заказ-нарядов. Диспетчерская информация представляется в той последовательности, в которой работа должна быть выполнена, и изменяется в реальном времени по мере возникновения событий на цеховом уровне. Это дает возможность изменения

заданного календарного плана на уровне производственных цехов. Включает функции устранения брака и переработки отходов наряду с возможностью контроля трудозатрат в каждой точке процесса с буферизацией данных.

4) DOC (англ. *Document Control*) – управление документами.

Контролирует содержание и прохождение документов, которые должны сопровождать выпускаемое изделие, включая инструкции и нормативы работ, способы выполнения, чертежи, процедуры стандартных операций, программы обработки деталей, записи партий продукции, сообщения о технических изменениях, передачу информации от смены к смене, а также обеспечивает возможность вести плановую и отчетную цеховую документацию. Включает инструкции по безопасности, контроль защиты окружающей среды, государственные и необходимые международные стандарты. Хранит историю прохождения и изменения документов;

5) DCA (англ. *Data Collection/Acquisition*) – сбор и хранение данных. Взаимодействие информационных подсистем в целях получения, накопления и передачи технологических и управляющих данных, циркулирующих в производственной среде предприятия. Функция обеспечивает интерфейс для получения данных и параметров технологических операций, которые используются в формах и документах, прикрепляемых к единице продукции. Данные могут быть получены с цехового уровня как вручную, так и автоматически от оборудования в требуемом масштабе времени;

6) LM (англ. *Labor Management*) – управление персоналом. Обеспечивает получение информации о состоянии персонала и управление им в требуемом масштабе времени. Включает отчетность по присутствию и рабочему времени, отслеживание сертификации, возможность отслеживания непроизводственной деятельности, такой как подготовка материалов или инструментальные работы, в качестве основы для учета затрат по видам деятельности (activity based costing, ABC). Возможно взаимодействие с функцией распределения ресурсов для формирования оптимальных заданий;

7) QM (англ. *Quality Management*) – управление качеством. Обеспечивает анализ в реальном времени измеряемых показателей, полученных от производства, для гарантированно правильного управления качеством продукции и определения проблем, требующих вмешательства обслуживающего персонала. Данная функция формирует рекомендации по устранению проблем, определяет причины брака путем анализа взаимосвязи симптомов, действий персонала и

результатов этих действий. Может также отслеживать выполнение процедур статистического управления процессом и статистического управления качеством продукции (SPC/SQC), а также управлять выполнением лабораторных исследований параметров продукции. Для этого в состав MES добавляются лабораторные информационно-управляющие системы (LIMS);

8) PM (англ. *Process Management*) – управление производственными процессами. Отслеживает производственный процесс, корректирует автоматически либо обеспечивает поддержку принятия решений оператором для выполнения корректирующих действий и усовершенствования производственной деятельности. Эта деятельность может быть как внутриоперационной и направленной исключительно на отслеживаемые и управляемые машины и оборудование, так и межоперационной, отслеживающей ход процесса от одной операции к другой. Она может включать управление тревогами для обеспечения гарантированного уведомления персонала об изменениях в процессе, выходящих за приемлемые пределы устойчивости. Обеспечивает взаимодействие между интеллектуальным оборудованием и MES, возможное благодаря функции сбора и хранения данных;

9) MM (англ. *Maintenance Management*) – управление техобслуживанием и ремонтом. Отслеживает и управляет обслуживанием оборудования и инструментов. Обеспечивает их работоспособность. Позволяет планирование периодического и предупредительного ремонтов, ремонта по состоянию. Накапливает и хранит историю произошедших событий (отказы, уменьшение производительности и др.) для использования в диагностировании возникших и предупреждения возможных проблем;

10) PTG (англ. *Product Tracking and Genealogy*) – отслеживание и генеалогия продукции. Обеспечивает возможность получения информации о состоянии и местоположении заказа в каждый момент времени;

11) PA (англ. *Performance Analysis*) – анализ производительности. Обеспечивает формирование отчетов о фактических результатах производственной деятельности, сравнение их с историческими данными и ожидаемым коммерческим результатом. Результаты производственной деятельности включают такие показатели, как коэффициент использования ресурсов, доступность ресурсов, время цикла для единицы продукции, соответствие плану и стандартам функционирования. Может включать статистический контроль качества про-

цессов и продукции (SPC/SQC). Систематизирует информацию, полученную от разных функций, измеряющих производственные параметры.

Основной инструмент при планировании бизнеса, позволяющий принимать решение, – это *отчетная документация*. Именно она является основой работы ERP, которая, в свою очередь, должна предоставлять возможность анализировать данные отчетов с различных позиций. Эти системы разделяются по способу хранения данных, виду организации, интерфейсу (рис. 3.13).

Рис. 3.13. Виды ERP-систем

ERP-система должна обладать рядом следующих функций:

– *обеспечение удобного документооборота.* Основным назначением ERP-систем является обеспечение быстрого оформления документации (счета, накладные, отчеты, прайсы), а также последующих операций с ними (поиск, доступ, пересылка, редактирование);

– *планирование*. Алгоритм системы, особенно для производства, должен позволять планировать платежи, поставки, работу склада, сезонные изменения, объемы продукции. Для каждой компании планирование производства носит индивидуальный характер и привязано к объемно-календарной стратегии;

– *прозрачность информации.* Программа должна фиксировать все операции, стороны, объемы и даты их проведения, что сделает работу компании более прозрачной для анализа;

– *разграничение доступа для разных уровней*. Поскольку система охватывает колоссальный объем информации о работе компании,

большая часть которой должна оставаться закрытой для сотрудников нижних уровней, клиентов и партнеров, она должна позволять закрывать часть данных для пользователей с различным допуском;

– *единая сеть данных.* ERP-система должна обеспечивать возможность отслеживать все процессы в отдельности (например, сделки) на всех уровнях – от закупки сырья и производства до оформления продажи и уплаты налога;

– *кадровый учет.* Программа должна предусмотреть возможность контроля численности персонала, планирование графика выходов и отработанных часов, учет уровня квалификации сотрудников и составление графиков отпусков, прохождение курсов повышения квалификации. Также эффективная система планирования предусматривает возможность расчета зарплат и премий с учетом формы оплаты труда;

– *работа с поставщиками.* Функционал системы должен позволять хранить и обрабатывать базу поставщиков, отправлять запросы на наличие, планировать формирование заказов, высвобождение оборотных средств и оплату счетов, контролировать процесс доставки, а также вести отчетность по закупкам;

– *работа с клиентами.* Система должна позволять вести полный учет данных по каждому клиенту, независимо от того, сколько юридических лиц входит в структуру последнего;

– *сервисное обслуживание и ремонт.* Если речь идет о производстве, эта часть программы должна обеспечивать планирование технического осмотра оборудования, графика проведения планового ремонта, модернизации или замены оснащения предприятия. Для торговых предприятий в системе должна быть предусмотрена возможность учета сервисного обслуживания проданных товаров и ремонта по гарантийным обязательствам.

Глава 4. Кибербезопасность и операционная эффективность

4.1. Нормативные документы по кибербезопасности Республики Беларусь

Цифровая трансформация современного общества в условиях информационной революции формирует новые угрозы информационной безопасности как отдельных государств, так и конкретных регионов. Актуальной данная проблема является и для государств-членов Организации Договора о коллективной безопасности, в том числе и Республики Беларусь.

В целях повышения уровня защиты национальной информационной инфраструктуры от внешних и внутренних угроз в соответствии с Указом Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» (15.02.2023, 1/20733) в Республике Беларусь создается национальная система обеспечения кибербезопасности (далее – система кибербезопасности).

Элементами системы кибербезопасности являются:

– Оперативно-аналитический центр при Президенте Республики Беларусь (далее – ОАЦ), который осуществляет координацию деятельности других государственных органов и иных организаций по созданию и функционированию системы кибербезопасности;

– создаваемый в структуре ОАЦ Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты (далее – Национальный центр кибербезопасности), функции которого определены Указом;

– центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций (далее – центры кибербезопасности), перечень которых определяется Советом Министров Республики Беларусь по предложению ОАЦ и подлежит ежегодной актуализации;

– оператор электросвязи по взаимодействию Национального центра кибербезопасности, центров кибербезопасности, а также государственных органов и иных организаций;

– объекты информационной инфраструктуры государственных органов и иных организаций (далее – объекты информационной инфраструктуры);

– сети передачи данных, используемые для взаимодействия элементов системы кибербезопасности.

Указом определены задачи системы кибербезопасности:

– достижение максимальной скоординированности действий государственных органов и иных организаций по обнаружению, предотвращению и минимизации последствий кибератак на объекты информационной инфраструктуры;

– постоянный поиск потенциальных уязвимостей национального сегмента глобальной компьютерной сети Интернет;

– проведение анализа информации о кибератаках и вызванных ими киберинцидентах, установление причин киберинцидентов;

– оценка эффективности защищенности объектов информационной инфраструктуры от кибератак;

– прогнозирование ситуации в области обеспечения кибербезопасности.

Для реализации функции реагирования на киберинциденты в составе Национального центра кибербезопасности создается и функционирует национальная команда реагирования на киберинциденты (CERT.BY).

Правовым актом предусмотрено, что владельцы критически важных объектов информатизации (37 организаций, указанных в приложении к Указу), а также уполномоченные поставщики интернет-услуг, оказывающие услуги хостинга официальных интернет-сайтов и электронной почты, обеспечивают создание центров кибербезопасности, функции которых определены Указом. Также центры кибербезопасности могут создаваться организациями, имеющими лицензии на деятельность по технической и (или) криптографической защите информации в части составляющих данный вид деятельности работ по проектированию, созданию, аудиту систем информационной безопасности критически важных объектов информатизации.

До начала функционирования центры кибербезопасности подлежат аттестации, проводимой ОАЦ.

Также в соответствии с Указом руководитель государственного органа и иной организации несет персональную ответственность за обеспечение кибербезопасности этого органа (организации).

Таким образом, Указом № 40 «О кибербезопасности» определяется правовая основа создания и функционирования национальной системы обеспечения кибербезопасности, предусматривающей формирование комплексного многоуровневого механизма противодействия кибератакам на государственные органы и организации, критическую информационную инфраструктуру. В частности, конкретизированы функции и задачи по обеспечению кибербезопасности государственных органов и иных организаций, закреплена персональная ответственность их руководителей, а также определены владельцы критически важных объектов информатизации, обеспечивающие первоочередное создание центров кибербезопасности. Указ направлен на дальнейшую реализацию положений Концепции национальной безопасности и взаимосвязан с Концепцией информационной безопасности. Реализация мер, предусмотренных в Указе, позволит консолидировать усилия по предотвращению, обнаружению и минимизации последствий кибератак на объекты информационной инфраструктуры, тем самым повысить безопасность и надежность информационных систем (https://president.gov.by/ru/documents/ukaz-no-40-ot-14-fevralya-2023-g).

Приведем нормативные правовые акты министерств, иных республиканских органов государственного управления:

– Государственная программа «Цифровое развитие Беларуси» на 2021–2025 годы, утвержденная постановлением Совета Министров Республики Беларусь от 2 февраля 2021 г. № 66;

– Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»;

– Указ Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет»;

– Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации»;

– Указ Президента Республики Беларусь от 23 января 2014 г. № 46 «Об использовании государственными органами и иными государственными организациями телекоммуникационных технологий»;

– Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» (https://mpt.gov.by/ru/news/13-03-2023-8311);

– Рекомендации государственным органам и иным организациям (в том числе владельцам критически важных объектов информатизации) по выполнению обязательных для исполнения требований за-

конодательства в сфере обеспечения кибербезопасности, в том числе технической и криптографической защиты информации (Оперативно-аналитический центр при Президенте Республики Беларусь. – Минск : Нац. центр кибербезопасности, 2025. – 76 с.).

Целью данной главы является формирование у магистрантов неинформационных специальностей общих представлений о безопасности в информационном обществе и на этой основе развитие навыков в области технологий информационной безопасности и умения применять правила кибербезопасности во всех сферах деятельности, а также совершенствование навыков ориентирования в информационных потоках, оценивание комплексного обеспечения информационной безопасности критической инфраструктуры объектов нефтегазовой отрасли, ознакомление с особенностями обеспечения информационной безопасности при работе в компьютерной сети и с программным обеспечением.

4.2. Общие понятия о кибербезопасности

Кибербезопасность – это практика защиты критически важных систем и конфиденциальной информации от цифровых атак. Меры кибербезопасности, известные как безопасность информационных технологий, предназначены для борьбы с угрозами в отношении сетевых систем и приложений, независимо от того, исходят ли эти угрозы из организации или извне.

Ее целью является обеспечение конфиденциальности, целостности и доступности информации, а также предотвращение нанесения ущерба компьютерным системам и пользователям.

Понятие «кибербезопасность» следует отличать от информационной безопасности: часто они используются в качестве синонимов, но на самом деле под кибербезопасностью понимается защита от атак в киберпространстве, а информационная безопасность занимается защитой данных (т. е. информации) от любых форм угроз – цифровых или аналоговых (рис. 4.1).

Домен. Кибербезопасность означает защиту всего и вся, что присутствует в киберсфере. Информационная безопасность касается защиты как цифровой информации, так и аналоговой.

Процесс. Кибербезопасность связана с защитой киберпространства и предотвращения кибератак. Информационная защита защищает информацию от любой формы угрозы.

Кибербезопасность касается киберпреступлений, кибермошенничества и правоохранительных органов.

Рис. 4.1. Общая схема элементов киберпространства

Основы и принципы кибербезопасности

Принцип конфиденциальности, т. е. гарантия того, что определенная информация не будет доступна несанкционированным лицам.

Принцип целостности данных, т. е. гарантия, что данные не будут изменены или заменены несанкционированно.

Принцип доступности, т. е. возможность для авторизованных пользователей воспользоваться данными или ресурсами в нужный момент.

Основные цели кибербезопасности:

1. Защита от хакерских атак, вредоносных программ и других киберугроз, которые могут нанести вред системе.

2. Обеспечение аутентификации и авторизации, т. е. предоставление права доступа только подтвержденным пользователям к соответствующей информации.

3. Безопасность сетевой инфраструктуры, серверов, устройств и программного обеспечения.

4. Операционная безопасность, т. е. обеспечение взаимодействий между системами и пользователями.

5. Повышение осведомленности пользователей о возможных угрозах, распространение информации о мерах защиты данных и систем.

6. Создание стратегии для выявления и реагирования на киберинциденты, чтобы минимизировать последствия, т. е. аварийное восстановление или планирование.

7. Соблюдение правил, нормативов и стандартов в области кибербезопасности.

4.3. Объекты защиты и задачи информационной безопасности в нефтегазовой отрасли

Производственные объекты нефтегазовой отрасли в любом ее сегменте – разведка и добыча, транспортировка, переработка или сбыт – технологически сложны, они оснащены множеством датчиков, генерирующих большие объемы данных. Растущая важность данных для крупнейших нефтегазовых компаний означает необходимость их защиты и внедрения эффективных систем информационной безопасности.

Кибербезопасность как неотъемлемую часть своей цифровой трансформации и обеспечения стабильной работы в целом рассматривает подавляющее большинство нефтегазовых компаний, являющуюся одним из главных приоритетов для газовой и нефтяной промышленности в связи с решающим значением отрасли для глобальной и национальной экономики.

IoT-устройства, объем передаваемых данных, интеграция новых ИТ-решений и АСУ ТП приводит к росту угроз кибербезопасности. Активы предприятий отрасли становятся объектами все большего числа изощренных атак, совершаемых как киберпреступниками, так и специальными службами отдельных государства. Компания, подвергшаяся атаке, может столкнуться с остановкой производства, повреждением оборудования, перебоями в работе внутренних служб и утечкой информации. Кроме того, последствия киберинцидентов могут выйти не только за рамки финансового ущерба и потери деловой репутации, но и повлиять на репутацию России, как стабильного производителя энергоресурсов. Перед лицом угроз кибербезопасности предприятиям отрасли необходимо понимать масштаб текущих рисков и определять оптимальные ответные меры. Не секрет, что АСУ ТП играют жизненно важную роль в каждой нефтегазовой компании, и фактически берут на себя большую часть автоматизации. Поэтому, помимо стандартных мер защиты информационных активов, следует рассматривать меры по обеспечению безопасности АСУ ТП.

Объекты защиты в нефтегазовой отрасли

К объектам защиты в нефтегазовой отрасли можно отнести как

производственные и коммерческие процессы (информация о месторождениях, запасах и исследованиях, характеристики продукции, результаты экономической деятельности), так и технологические процессы (АСУ ТП и информационная инфраструктура).

Задачи информационной безопасности в нефтегазовой отрасли:

– защита АСУ ТП;

– обеспечение безопасности корпоративных ресурсов (информационная инфраструктура, веб-ресурсы);

– защита конечных устройств;

– защита чувствительной информации и персональных данных;

– соответствие требованиям регуляторов;

– предотвращение утечек информации;

– выявление внутренних злоупотреблений и нелояльных сотрудников.

Решения кибербезопасности для нефтегазового сектора:

– регулярные тренинги – для повышения осведомленности персонала в вопросах информационной безопасности;

– аудит информационной безопасности и инструменты сканирования сети для обнаружения и предотвращения эксплуатации уязвимостей, своевременного патчинга;

– корректная сегментация сети – для лучшего контроля сетевого трафика и повышения эффективности систем кибербезопасности;

– системы защиты АСУ ТП – для поддержания непрерывности технологического процесса;

– NTA (Network Traffic Analysis) – для обнаружение аномалий в трафике и выявления кибератак на ранних этапах;

– межсетевые экраны и системы обнаружения и предотвращения вторжений (IDS/IPS) – для защиты периметра сети, блокировки несанкционированного доступа и обнаружения потенциально вредоносного трафика;

– WAF (Web Application Firewall) – для защиты веб-ресурсов с помощью межсетевых экранов приложений от таких атак, как межсайтовая подделка запроса (CSRF), межсайтовый скриптинг (XSS), SQL-инъекция и других угроз;

– защита конечных точек для снижения риска заражения программами и вирусами, шифрования информации, соблюдения соответствия политикам и регламентам информационной безопасности;

– организация безопасного удаленного доступа к сети и создания зашифрованного канала связи с помощью средств криптографической защиты информации (СКЗИ) и VPN;

– СЗИ от НСД – для защиты стационарных и мобильных устройств от несанкционированного доступа, а также обеспечения соответствия требованиям регуляторов;

– DLP-системы – для предотвращения утечки конфиденциальных материалов, а именно анализа и блокировки данных, передаваемых с помощью электронной почты, мессенджеров, интернет-ресурсов и других источников;

– системы управления доступом (IDM, PIM) – для контроля жизненного цикла учетных записей и разграничения прав доступа к сегментам сети;

– решения для управления сетевым доступом (NAC) – для инвентаризации устройств, обеспечения видимости и контроля подключений к корпоративной сети;

– системы классификации данных – для повышения безопасности конфиденциальной информации путем классификации, определения пользователей, взаимодействовавших с документами, упрощения доступа, поиска и отслеживания данных, а также устранения дублирований;

– использование интерактивных ловушек для эффективного обнаружения APT-атак;

– SIEM-системы – для централизованного мониторинга информационной безопасности, сбора и анализа данных от инструментов кибербезопасности.

Только многоуровневый подход к информационной безопасности обеспечит оптимальную защиту как информационных активов, так и систем автоматизации производства предприятий отрасли.

Все нефтяные компании рассматривают кибербезопасность как инструмент обеспечения эффективности своей деятельности и гарантию защиты своей интеллектуальной собственности.

Нарушения требований кибербезопасности является одним из наиболее приоритетных рисков, представляющих угрозу для цифровой инфраструктуры, промышленных систем управления и операций. Есть большая вероятность того, что кибератаки будут нацелены на ее поставщиков, чтобы получить доступ к информации или системам, поэтому следует вести работу со своими контрагентами, разделяя роль по защите информации и систем.

Многие компании подвергаются многочисленным и постоянно меняющимся рискам кибербезопасности, в том числе атакам хакеров, вторжениям, спонсируемым государствами, промышленному шпиона-

жу и др. Эти киберугрозы как внутренние, так и внешние становятся все более изощренными и скоординированными. Поэтому предприятия нефтегазовой отрасли выделяют значительные ресурсы для предотвращения нежелательных вторжений и защиты своих систем и данных.

Разрабатываются стратегии киберустойчивости, включающие две основные части:

– обеспечение эффективной защиты от возможных угроз и нарушений безопасности;

– план восстановления мощностей в случае возникновения сбоев для поддержания непрерывности бизнеса.

Также предприятия свой подход к обеспечению кибербезопасности основывают на управлении рисками и соблюдении национальных и глобальных нормативных требований. Этот подход отражен в централизованном управлении кибербезопасностью, четкой организации процессов защиты, регулярных аудитах и проверках для тестирования принятой модели информационной безопасности, а также во внедрении административных, технических и физических средств контроля над угрозами кибербезопасности.

4.4. Методы обеспечения безопасности персональных компьютеров и Интернета, вирусы и антивирусы

Вредоносное ПО (malware) – это программы, которые нарушают работу устройств, непосредственно выполняют деструктивную функцию, крадут данные или получают несанкционированный доступ к личным данным, включая логины и пароли. Его ключевая особенность – целенаправленная вредоносность. В отличие от багов, которые возникают случайно, вредоносное ПО изначально создается для конкретных задач (рис. 4.2).

Вредоносное ПО эволюционирует. Если раньше вирусы просто удаляли файлы, то сегодня они используют ИИ для анализа поведения жертв. Например, троян Cerberus подменял интерфейсы мобильных банков фальшивыми экранами ввода паролей, анализировал поведение пользователей и таким образом получал вводимые ими логины, пароли и другие личные данные.

Рассмотрим, как работают вредоносные программы. Вредоносное ПО – это не просто код. Это сложный механизм, в котором сочетаются как технические, так и психологические уловки. Кибератаки проходят пять основных этапов:

1) *проникновение* – обычно это происходит через фишинговые письма или уязвимости в ПО;

2) *активация* – вирус может «спать» месяцами и включиться в самый подходящий для злоумышленников момент;

3) *заражение* – например, черви самостоятельно распространяются по сети;

4) *выполнение задачи* – здесь происходит непосредственно преступление: кража данных, шифрование файлов, создание ботнета и др.;

5) *сокрытие следов* – некоторое вредоносное ПО может маскироваться под системные службы и процессы, в результате чего жертва долгое время остается в неведении.

Рис. 4.2. Классификация вредоносных программ https://cf.ppt-online.org/files/slide/s/slide-15.jpg.

Так, в 2025 г. «Лаборатория Касперского» обнаружила мобильный троян SparkCat. Он скрывался в 20 фейковых приложениях из AppStore и Google Play под видом мессенджеров и ИИ-ассистентов. Троян крадет данные с фотографий на смартфоне – анализирует текст на изображениях и т. п. Все это используется для дальнейшей кражи денег.

Основные типы вредоносных программ

Каждый тип вредоносного ПО имеет свои особенности и цели (рис. 4.3). Рассмотрим ниже наглядные примеры.

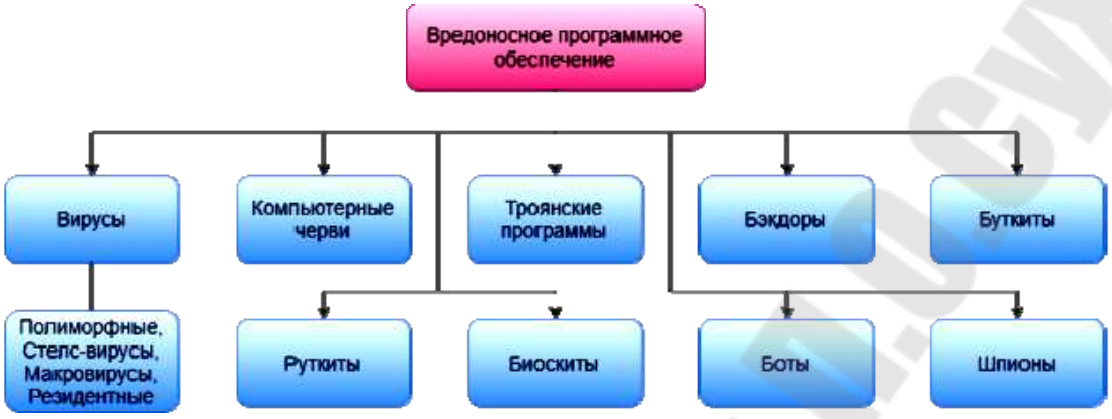

Рис. 4.3. Типы вредоносного программного обеспечения

1. Вирусы

Обычно прикрепляются к файлам и активируются при их запуске. Способны мутировать, усложняя обнаружение. Самый известный пример – ILOVEYOU из далекого 2000 г. Этот вирус рассылался в виде письма с признанием в любви. Финальный ущерб оценивается в $15 млрд.

Современные макровирусы часто внедряются в Excel-документы через макросы. Также они находятся в ZIP-архивах при скачивании программ, особенно нелицензионных или пиратских.

2. Трояны

Трояны – вредоносные программы, которые маскируются под полезные приложения, чтобы обмануть пользователя. В отличие от вирусов, они не размножаются сами, но открывают «черный ход» для хакеров. Попадая в систему, трояны крадут пароли, банковские данные или превращают устройство в часть ботнета. Например, троян Emotet выдавал себя за документ Word, а затем похищал конфиденциальную информацию. Главная опасность троянов – их способность оставаться незамеченными.

3. Черви

Черви – это вредоносные программы, которые распространяются по сети без участия пользователя. В отличие от вирусов, они не нуждаются в прикреплении к другим файлам. Черви используют уязвимости в ПО или социальную инженерию, чтобы заражать устройства. Их главная опасность – скорость распространения.

Например, в 2025 г. российские организации из сферы телекоммуникаций и промышленности стали мишенью новой версии червя Merlin, который крадет конфиденциальные данные. Атаки распространяются через фишинговые письма. Например, одно из них было адресовано отделу кадров машиностроительного завода с просьбой предоставить характеристику на бывшего сотрудника. В письме содержалась вредоносная ссылка на архив с якобы резюме, который запускал заражение.

4. Шпионские программы

Шпионские программы – вредоносное ПО, которое тайно собирает данные с устройства: пароли, переписку, историю браузера и многое другое. Они маскируются под легитимные приложения или внедряются в систему через уязвимости. Например, Pegasus – одна из самых известных шпионских программ, которая следила за журналистами и активистами через iPhone, активируя камеру и микрофон без ведома владельца.

5. Рекламные программы (Adware)

Adware – это вредоносное ПО, которое навязывает рекламу, замедляет работу устройства и перенаправляет трафик на сомнительные сайты. Оно часто маскируется под бесплатные приложения или расширения для браузера. Например, Fireball – одна из самых известных рекламных программ, захватила 250 млн компьютеров, подменяя поисковики и устанавливая прокси-серверы. Главная проблема Adware – не только раздражающая реклама, но и риск утечки данных, так как оно собирает информацию о всей интернет-активности пользователя.

6. Ransomware

Ransomware шифрует файлы и требует выкуп. Из последних громких случаев – UnitedHealth Group, которая стала жертвой масштабной атаки. Злоумышленники зашифровали систему и похитили данные 190 млн человек. Компания понесла убытки в $3,09 млрд, дважды выплатив выкуп хакерам.

7. Ботнеты

Ботнет – это сеть компьютеров, смартфонов или других устройств, зараженных вредоносным ПО. Эти устройства называются «ботами» и используются для массовых атак, таких как DDoS (перегрузка серверов), рассылка спама или майнинг криптовалюты.

Главная опасность ботнетов – их масштаб и скрытность. Владельцы зараженных устройств часто даже не подозревают, что их техника используется для киберпреступлений. Например, в 2023 г. ботнет Mirai

атаковал серверы крупных компаний, включая Amazon и Google. Это вызвало масштабные сбои в работе интернет-сервисов. Злоумышленники использовали уязвимости в IoT-устройствах (камеры, роутеры), чтобы создать армию из миллионов зараженных устройств.

8. Руткиты

Руткиты – вредоносные программы, которые маскируются под системные процессы или файлы. Это позволяет им скрыть свое присутствие и действия в зараженной системе. Руткиты предоставляют злоумышленникам почти полный контроль над устройством.

В 2022 г. руткит Sliver был обнаружен в корпоративных сетях по всему миру. Он использовался хакерами для скрытого доступа к серверам и кражи конфиденциальной информации. Sliver маскировался под легитимные системные файлы, что затрудняло его обнаружение даже продвинутыми антивирусами.

9. Бэкдоры (backdoor)

Бэкдоры – общее наименование для целого ряда методик взлома путем вживления в операционную систему специальных аппаратных либо программных дополнений для получения доступа информации, хранящейся в базах данных. Имеется несколько путей проникновения внутрь системы:

– в обычную программу, не вызывающую никаких подозрений у хозяина компьютера, встраивается вредоносный код или вирус, дающий мошенникам возможность пользоваться данными с девайса, на котором активирована данная программа. При этом жертва в начале даже не «забьет тревогу», так как работа ПК не будет ничем настораживать;

– в аппаратную часть того устройства, с которого осуществляется выход во Всемирную сеть (чаще всего роутера) вставляется микроскопическая плата с кодом, который открывает доступ ко всем файлам и программам, хранящимся в памяти. Далее файл сам подменяет все коды на вредоносные. В итоге информация оказывается в свободном доступе.

10. DoS-атаки

DoS-атаки – такие киберугрозы действуют при помощи намеренной поломки одного или нескольких корпоративных устройств. Чаще всего зараженные технические средства реагируют на манипуляции хакеров кратковременными перебоями в работе, чего зачастую хватает для поражения инфохранилищ. При полном доступе к системе программисты либо сразу загружают нужные файлы на собственные носители, либо заражают систему вирусом, который делает это за

них. Бэкдоры в этом случае хороши тем, что их активацию можно провести удаленно.

Другой вид такой атаки заключается в предумышленной блокировке аккаунтов на важных сайтах после неправильного подбора пароля и логина хозяином. В результате этого пользователь не может войти и бросает все попытки это сделать. Цель такой атаки – воздействовать на нервное состояние жертвы. Здесь прежде всего целью является порча репутации и доброго имени конкурирующего предпринимателя с умыслом обелить собственную биографию. Многим хакерам проведение таких схем заказывают участники конкурентных войн.

11. Перехват сетевого трафика

Эта схема используется тогда, когда мошенники не могут проникнуть в сеть напрямую. Суть в том, что при помощи специального программного обеспечения злоумышленники генерируют фальшивые точки раздачи Интернета, называя их так же, как привычные для работника. Заходя на них, наивный сотрудник открывает преступникам огромный простор для действий. В итоге вся секретная информация находится в их руках.

12. Фишинг

Фишинг – на электронную почту пользователя приходит любопытное письмо, говорящее о щедром вознаграждении либо выигрыше в лотерею. В этом письме находится ссылка, открыв которую, счастливчик попадает на сайт с формой для указания реквизитов карт для перевода. Естественно, никто ничего не получает, а деньги уходят как вода сквозь пальцы.

13. Социальная инженерия

У специалистов по кибербезопасности есть веские основания считать человеческий фактор наислабейшим аспектом защиты. Этим активно пользуются и преступники, применяя все возможности социальной инженерии для того, чтобы получить любые персональные данные для них.

Чтобы вызвать доверие, «охотники за деньгами» притворяются сотрудниками банковских организаций, проводящими прозвон клиентов. Если жертва не верит, мошенник добавляет, что звонит с целью актуализации номера в базе.

14. Спуфинг

Спуфинг заключается в том, чтобы, заходя под разными IP-адресами, выманивать у других пользователей полезную для себя информацию. Для этого они предпринимают следующие действия:

– подменяют IP/MAC-адрес своего гаджета, чтобы войти в сеть, где имеется файрвол с возможностью фильтрации IP/MAC-адресов;

– фальсифицируют электронные письма для рассылки, указывая тот адрес, который заслужил у пользователя доверие;

– обманывают путем подмены номера телефона в рассылке на тот, который похож на реальный, но не является таковым.

Спуфинг и **фишинг** построены на сходных приемах, которые опираются на социальную инженерию. Цель преступников в данном случае проста, как мир – узнать секретную информацию о жертве путем доверительного общения.

Тайпсквоттинг/кибersквоттинг

Тайпсквоттинг/кибersквоттинг – схема кибермошенничества, основанная на человеческой рассеянности. Регистрируя поддельные домены, очень похожие на настоящие, мошенники надеются, что жертва из-за своей невнимательности допустит ошибку при введении (к примеру, пропустит точку). Теперь все очень просто: не заметив своей ошибки, пользователь заходит на сайт, чей интерфейс с точностью повторяет вид настоящего сайта, вводит данные своей карты либо кошелька и все средства уходят в руки аферистов.

Отличие этой схемы обмана от предыдущих в том, что для ее реализации не требуется проводить никаких рассылок. Главное здесь – дождаться допущенной при наборе адреса ошибки.

Признаки заражения вредоносными ПО

Даже скрытое вредоносное ПО оставляет следы. Важно следить за работой компьютера (смартфона) и своевременно принимать меры. Вот как вредоносное ПО выдает себя:

• *Неожиданные всплывающие окна и реклама.* Появление рекламы в необычных местах (например, на рабочем столе или в какой-то программе) и перенаправление на подозрительные сайты является признаком вредоносного ПО.

• *Необъяснимая нагрузка на процессор или видеокарту.* Майнеры активно используют ресурсы видеокарты. Если в данный момент на компьютере не запущено никакое требовательное к ресурсам приложение (современная игра с 3D-графикой, рендеринг видео или 3D-моделирование), это верный признак работы майнера.

• *Неизвестные программы и процессы.* В списке установленных программ появляются приложения, которые вы не устанавливали. В диспетчере задач будут неизвестные процессы с высоким потреблением ресурсов.

• *Браузер сам открывает вкладки*. Обычно это реклама незаконных казино, букмекеров или фейковых конкурсов. Явный признак заражения устройства.

• *SMS с кодами подтверждения*. Это значит, что злоумышленники пытаются взломать какой-то из ваших аккаунтов. Ни в коем случае никому не называйте эти коды.

• *Сообщения в мессенджерах в стиле* «Это ты на видео?» или «Видел, где тебя опубликовали?». С недавнего времени в России распространяется вирус Mamont, который нацелен на пользователей Android-смартфонов. Его цель – заставить человека установить вредоносный файл, который предоставит мошенникам доступ к банковским приложениям.

Как удалить вредоносное ПО с устройств

1. С компьютера (Windows) – отключите Интернет. Так можно предотвратить передачу данных злоумышленникам.

2. Загрузите ПК в безопасном режиме (Shift + Restart → «Поиск и устранение неисправностей» → «Дополнительные параметры» → «Параметры загрузки»).

3. Просканируйте систему разными инструментами по очереди (это значительно увеличит шансы найти вредоносное ПО):

– Malwarebytes – против троянов и шпионов;

– HitmanPro – для поиска руткитов;

– AdwCleaner – удаляет Adware.

4. Очистите автозагрузку через диспетчер задач или утилиту Autoruns. Удалите оттуда все программы и процессы, которые не нужны при запуске ПК. Сбросьте браузеры. Удалите расширения, очистите кэш и cookie.

Способы защиты от вредоносных программ в Интернете

Антивирусные ПО – это первая линия защиты от большинства вредоносных программ. Они блокируют вирусы, трояны, червей и другие угрозы (например, Kaspersky, Avast, Malwarebytes).

Регулярно обновляйте базы данных и проводите полное сканирование системы.

Используйте встроенные функции, такие как защита от фишинга и сетевых атак.

Относитесь к вложениям и ссылкам с подозрением

Многие вредоносные программы распространяются через фишинговые письма и подозрительные файлы.

Не открывайте вложения и не переходите по ссылкам от неизвестных отправителей.

Используйте облачные сервисы (например, Google Диск) для просмотра подозрительных файлов – это снижает риск заражения.

Проверяйте адреса отправителей. Злоумышленники часто маскируются под известные компании и использую почтовые адреса в стиле «pr@sberbakn.ru» (перепутаны символы), «info@gosuslug.ru» (пропущен 1 символ) и «director@beel1ne.ru» (единичка вместо буквы "i" и должность директора, которая должна внушать доверие).

Регулярно обновляйте ПО

Устаревшие программы – это лазейка для хакеров. Обновления часто содержат исправления уязвимостей, поэтому их нельзя игнорировать.

Включите автоматическое обновление операционной системы и приложений (актуально для любых платформ, включая Windows, MacOS, Android, iOS и даже Linux). Не игнорируйте обновления для браузеров, антивирусов и офисных программ. Они часто становятся объектом хакерских атак.

Используйте двухфакторную аутентификацию (2FA)

Даже если злоумышленники украдут пароль, двухфакторная аутентификация 2FA затруднит доступ к аккаунтам, поскольку потребует ввода одноразового кода, который придет на телефон или другое устройство настоящего владельца.

Например, в 2022 г. хакеры взломали аккаунты сотрудников Uber, но не смогли получить доступ к корпоративным системам благодаря 2FA.

Используйте менее популярные операционные системы

Многие вредоносные программы нацелены на Windows и Android. Переход на менее распространенные операционные системы (например, Linux или ChromeOS) снижает риск заражения. Если работа позволяет и есть определенные навыки администрирования, установите Linux (Ubuntu). Также можно пользоваться виртуальными операционными системами для запуска и тестирования подозрительных файлов.

Какие же принципы защиты наиболее удобны?

Обновления операционной системы и антивируса, чтобы закрывать уязвимости.

Антивирус. На Windows 11 использовать встроенный Microsoft Defender, которого достаточно в большинстве случаев.

Безопасные источники. Загружать программы только с официальных сайтов и проверенных ресурсов.

Проверка файлов. Не открывать подозрительные вложения и перед запуском проверять файлы через VirusTotal.

Бэкапы. Всегда делать резервные копии данных: вручную и в облаке (https:// Вредоносное ПО – каким бывает и как с ним бороться// hi-tech.mail.ru/review/129033-vredonosnoe-po/#anchor17503460842078100 7).

4.5. Информационная безопасность вычислительных сетей

Создаваемые масштабные компьютерные линии – локальные, корпоративные, телекоммуникационные – ставят задачу взаимодействия большого количества компьютеров, серверов, сетей и подсетей. Создается проблема определения наиболее эффективного метода защиты информации.

Системная топология, основанная на расположении межкомпьютерных связей, остается главным компонентом всех локальных и корпоративных сетей. Безопасность данных в компьютерных сетях достигается путем обработки критической информации. Этим термином обозначаются факторы, способствующие эффективному управлению основными структурными элементами сети и максимально полному выполнению стратегических задач любого уровня секретности (для личного, служебного пользования, коммерческая тайна либо интеллектуальная собственность физического или юридического лица).

Уязвимость большинства информационных сетей связана с кабельной системой. Есть данные, что именно она становится причиной сбоев и нарушений функционирования. Это необходимо учитывать уже на стадии проектирования сетевых связей.

Широкое распространение получили так называемые структурированные системы кабелей. Принцип их устройства – наличие однотипных проводов для передачи всех видов информации (цифровой, телефонной, видео, сигналов систем охраны).

Структурированность заключается в возможности разделить всю систему кабелей на ряд уровней по их назначению и наличию различных компонентов: внешней, администрирующей, аппаратной, магистральной, горизонтальной подсистем (Защита информации в компьютерных сетях. – URL: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/v-setyakh/v-kompyuternykh-setyakh/).

Решая вопрос защиты информации в корпоративных сетях, стоит обратить внимание на возможные перебои и нарушения в процессе доступа, способные уничтожить или исказить сведения.

Возможные проблемы, связанные с нарушением безопасности в компьютерных сетях, можно условно разделить на несколько типов:

– нарушение работы системного оборудования: разрыв кабелей, перебои в электропитании, сбой в дисковой системе, нарушение функционирования серверов, сетевых карт, рабочих станций, системы архивации;

– уничтожение данных вследствие некорректной работы ПО: ошибки системы, заражение компьютерными вирусами;

– следствие несанкционированного доступа: пиратское копирование, устранение или фальсификация данных, работа посторонних с секретными материалами;

– неграмотное сохранение архивов;

– ошибки технического штата и пользователей сетевого ресурса: случайное искажение либо уничтожение информации, некорректное пользование программными продуктами.

Сетевая безопасность в широком смысле – это прикладная научная дисциплина и целая отрасль информатики, которая занимается вопросами обеспечения безопасности сети. В узком смысле под сетевой безопасностью понимают комплекс методов и инструментов, которые обеспечивают защиту сетей от несанкционированного доступа, кибератак и других угроз. Чаще атакам подвергаются госучреждения (18 %), промышленные (11 %) и телекоммуникационные предприятия (10 %) (рис. 4.4).

Рис. 4.4. Распределение типов кибератак
Источник: ptsecurity.

С прикладной точки зрения понятие информационной безопасности включает изучение возможных способов атак на сети, серверы и личные данные пользователей. Другая важная составляющая обеспечения сетевой безопасности — освоение инструментов и способов предотвращения кибератак и защиты от них.

Задачи сетевой безопасности:

– блокировка несанкционированного доступа к сетевым ресурсам;

– обеспечение конфиденциальности, целостности и доступности данных;

– защита сетевых устройств от вредоносных атак;

– соответствие законодательству и нормативам по защите данных.

Рассмотрим угрозы сетевой безопасности:

● **Вирусы и вредоносное ПО.** Предназначенное для уничтожения, кражи или передачи данных ПО может быть внедрено в систему через зараженные файлы, ссылки или сетевые подключения.

● **Фишинг.** Использование обманных сообщений и веб-сайтов с целью кражи учетных данных и финансовой информации пользователя.

● **DDoS-атаки.** Цель таких атак – перегрузка сетевых ресурсов, которая может привести к их недоступности.

● **Несанкционированный доступ.** Попытки злоумышленников получить доступ к сетевым ресурсам с использованием уязвимостей в системах безопасности.

Более половины похищенной в результате кибератак на компании информации – это персональные данные и сведения, составляющие коммерческую тайну (*Источник*: ptsecurity).

Уровни сетевой безопасности

● **Физическая безопасность.** Это защита физических компонентов сетевой инфраструктуры, таких как серверные комнаты, где размещаются критически важные данные и оборудование.

● **Сетевая безопасность.** Защита самой сети, включая использование файрволов, антивирусов, средств мониторинга сети, сервисов аутентификации и т. д.

● **Прикладная безопасность.** Защита работающих в сети приложений и сервисов для предотвращения уязвимостей на уровне ПО.

● **Безопасность данных.** Применение шифрования и других мер для защиты конфиденциальных данных.

● **Управление инцидентами.** Это процессы и процедуры, направленные на быстрое реагирование на инциденты безопасности, – алёрты и т. д.

Важно понимать, что сетевая безопасность – это процесс, который требует постоянного мониторинга и совершенствования.

Инструменты обеспечения сетевой безопасности, которые помогают успешно справиться с различными видами угроз:

● **Файрволы, или межсетевые экраны.** Первая линия защиты сетевой инфраструктуры – образно говоря, огненная стена, которая стоит между пользователем и хакером или хакером и серверами. Файр-

волы контролируют входящий и исходящий сетевой трафик на основе заранее установленных правил. При попытках несанкционированного доступа или эксплуатации уязвимостей файрвол должен защитить сервера.

● **Системы предотвращения вторжений (IPS).** Системы IPS анализируют сетевой трафик в реальном времени и могут блокировать подозрительные действия, выявляя и предотвращая угрозы до того, как они нанесут вред системе.

● **Системы обнаружения вторжений (IDS).** IDS-технологии работают аналогично IPS, но лишь уведомляют администраторов о наличии подозрительной активности, не блокируя ее автоматически. Это позволяет проводить более тщательный анализ инцидентов после их возникновения.

● **Антивирусы.** Антивирусные программы сканируют файлы и программы на предмет наличия вредоносного ПО и помогают предотвратить его заражение. Регулярные обновления баз данных о вирусах и вредоносных программах обеспечивают актуальную защиту.

● **Управление доступом.** Управление доступом включает использование многофакторной аутентификации и других методов, которые проверяют и контролируют, кто может получать доступ к ресурсам сети. Это помогает минимизировать риски, связанные с несанкционированным доступом.

● **Пенетрейшн-тесты.** Проверка сетевой безопасности путем тестирования на проникновение, когда сотрудник или внешний аудитор играет роль внешнего пользователя или хакера и пытается найти уязвимости в системе. Инструмент включает анализ различных зависимостей, проверку самого кода на безопасность и симуляцию нагрузки, например, когда огромное количество пользователей одновременно пытаются сделать заказ.

● **Сканеры уязвимости** – специальные внешние инструменты для мониторинга и выявления слабых мест в информационной архитектуре. Их использование помогает заранее принять меры по устранению возможных уязвимостей, через которые хакеры могут атаковать.

● **Контейнеризация и визуализация** – технологии, которые позволяют отделить доступ к различным компонентам системы и помогают запустить приложения и сервисы таким образом, что в случае взлома страдает только часть системы, а не вся система в целом.

● **Sandbox, или «песочница».** Среда безопасного тестирования программ, полученных от клиентов файлов и т. д.

Решать проблему сетевой безопасности можно не на уровне антивирусов, а на уровне доступов, ограничивая возможности разных специалистов. Если у сотрудника нет доступа к определенной базе, никакой вирус не сможет ей воспользоваться.

Обеспечение сетевой безопасности в компании базируется на системном подходе, комбинацией наиболее подходящих инструментов на всех уровнях защиты, а именно:

● **Обучение сотрудников.** Если каждый сотрудник компании знает, как избежать фишинговых атак и других угроз, риск утечки данных для компании значительно ниже. Регулярные тренинги помогут поддерживать высокий уровень осведомленности сотрудников, а значит, и безопасности данных компании.

Политика безопасности. Компании необходимо разработать правила, которые четко регламентируют, как сотрудники должны использовать информационные ресурсы и как действовать в случае возникновения инцидентов.

● **Регулярный мониторинг.** Аудиты и тестирования на проникновение позволят оценить уровень сетевой безопасности компании, выявить уязвимости и вовремя принять меры.

● **Анализ рисков.** Оценка рисков и управление ими помогут идентифицировать возможные уязвимости и угрозы и принять проактивные меры по их минимизации.

4.6. Комплексный подход к промышленной кибербезопасности

АСУ ТП, или автоматизированная система управления технологическим процессом, в частном случае обеспечивает комплексную автоматизацию производства, выработку электроэнергии, добычу полезных ископаемых, переработку материалов, подачу и очистку воды или воздуха, управление ядерной энергетикой.

В качестве основных частей АСУ ТП можно выделить:

– САУ – системы автоматического управления;

– SCADA – диспетчерское управление и сбор данных;

– ESD – системы противоаварийной защиты;

– DCS – распределенные системы управления.

Физически они представлены рабочими местами инженеров АСУ ТП (рабочая станция в виде персонального компьютера), пультами управления, средствами и системами обработки поступающей

информации, датчиками, контроллерами, исполнительными устройствами, телеметрией. Текущая стадия развития АСУ ТП позволяет исключить человеческий фактор из многих процессов, нивелировав роль инженера-оператора и возложив на него функцию контроля без непосредственного вмешательства в технологический процесс, позволяя сделать последний максимально автономным.

С усложнением АСУ ТП появилась необходимость защиты их инфраструктуры и смежных систем. В частности, если раньше было возможно выделить АСУ ТП в особый сегмент сети, использовав так называемый «воздушный зазор» (air gap), то сейчас построить подобную схему очень трудно, особенно если это касается распределенных сетей, таких как сети городских электростанций, общественного транспорта, АЭС, ГЭС, т. е. сетей, разные части которых физически распределены, но без взаимосвязи не могут комплексно сопровождать единый технологический процесс, наполняя его информацией, регистрируя события, метрики, аварии, аномалии и иные взаимосвязанные сигналы, компенсируя нагрузку и обеспечивая бесперебойность процесса и устойчивость к катастрофам.

Для любой АСУ ТП рано или поздно возникнет необходимость обновления, съема данных, загрузки информации, установки нового ПО.

Однако возникают вопросы по внутренним нарушителям, отсутствию или недостатку контроля физического доступа, угроз в цепочке поставок, программных закладок в поставляемом ПО для АСУ ТП.

Несанкционированные или неконтролируемые подключения сети АСУ ТП к иным сетям, когда фактически никакого «воздушного зазора» в организации не существует, персонал подключает 3G-модемы к рабочим местам, сторонние подрядчики получают сетевой доступ в рамках сопровождения и обслуживания устройств и систем АСУ ТП, сами устройства или рабочее место оператора имеют беспроводные сетевые модули и могут подключаться к неконтролируемым точкам доступа, в том числе по Bluetooth.

Большая часть объектов управления АСУ ТП подпадает под определение критической информационной инфраструктуры (КИИ).

Ниже приведены основные требования к защите сетей АСУ ТП на протяжении всего жизненного цикла системы, в том числе:

– идентификация и аутентификация (ИАФ);
– управление доступом (УПД);
– ограничение программной среды (ОПС);
– защита машинных носителей информации (ЗНИ);
– аудит безопасности (АУД);

– антивирусная защита (АВЗ);

– предотвращение вторжений и компьютерных атак (СОВ);

– обеспечение целостности (ОЦЛ);

– обеспечение доступности (ОДТ);

– защита технических средств и систем (ЗТС);

– защита информационной (автоматизированной) системы и ее компонентов (ЗИС);

– планирование мероприятий по обеспечению безопасности (ПЛН), управление конфигурацией (УКФ);

– управление обновлениями программного обеспечения (ОПО);

– реагирование на инциденты в информационной безопасности (ИНЦ);

– обеспечение действий в нештатных ситуациях (ДНС);

– информирование и обучение персонала (ИПО).

Также есть нормативное требование: субъект КИИ должен сам проводить категорирование своих систем, но нередко у предприятий недостаточно внутренних компетенций для оценки рисков и угроз.

Одно из этих требований сводится к тому, что поставщик решения для АСУ ТП должен иметь у себя регламентированные процессы безопасной разработки. Международные вендоры, такие как Schneider Electric или Siemens, внедрением подобных механизмов уже занялись в соответствии с международным стандартом МЭК 62443-4-1 «Сети промышленной коммуникации. Безопасность сетей и систем». Помимо этого есть стандарт МЭК 61850 «Сети и системы связи на подстанциях» и нормативный документ ISA/IEC-62443, который описывает процедуры внедрения электронно-защищенных промышленных систем автоматизации и управления.

Выделим основные тенденции, которые увеличивают влияние общеизвестных угроз ИБ на сети АСУ ТП:

• **Развитие предприятий.** Старые системы управления, которые разрабатывались десятки лет назад и имеют неисправленные уязвимости, интегрируются в современные системы и сети (Windows, Linux, БД, Ethernet), которые и сами могут содержать бреши. Итоговый эффект неизвестен и может привести к негативным последствиям.

• **Усложнение технологических процессов.** Полная или частичная автоматизация даже самых простых процессов может привести к сбою большей части производственного процесса из-за программной ошибки, изъянов в логике при нештатных ситуациях, человеческого фактора, действий злоумышленника.

• **Доступность информации об АСУ ТП.** Все большее количество специалистов работают в обслуживании, управлении, продажах, сопровождении, внедрении систем АСУ ТП; соответственно, и информации о таких системах стало в сотни раз больше, чем 10 лет назад, когда ими занимались отдельные специалисты, часто с доступом к государственной тайне.

• **Удаленный доступ.** Уже ставший повседневным источник угроз как для рядового состава сотрудников предприятия, работающих из дома, так и для инженеров обслуживания систем управления, имеющих доступ к технологическому процессу.

Опишем проблемы внедрения кибербезопасности в АСУ ТП.

Во-первых, это малочисленность специалистов, занимающихся информационной безопасностью именно в АСУ ТП и разбирающихся в специфике рынка и технологиях.

Во-вторых, это нехватка на предприятии с АСУ ТП персонала, который занимался бы организацией защиты не только критически важного производственного контура, но и пользовательских сетей, серверной инфраструктуры.

В-третьих, это высокие затраты на закупку решений по безопасности АСУ ТП, которые сдерживают рост рынка.

4.7. Мониторинг инцидентов кибербезопасности

Безумный рост численности продвинутых угроз (APT) и такой же рост объема данных, нуждающихся в обработке для обнаружения атак, с каждым днем затрудняет работу аналитиков безопасности. В последние годы работа инженера по информационной безопасности часто заключается в ручном просеивании сотен предупреждений в попытках найти реальные угрозы. Из-за информационных массивов, которые генерируют организации, команды с ручным поиском угроз уже неэффективны. На борьбу с этой проблемой используются ресурсы и программные средства, но часто внедрение новых инструментов тормозится при интеграции в инфраструктуру организации. Поэтому каждой организации необходимо вырабатывать долгосрочную стратегию по защите своих данных от киберинцидентов. Стратегический цикл кибербезопасности компании приведен на рис. 4.5.

Рис. 4.5. Стратегический цикл кибербезопасности компании

Рассмотрим шесть наиболее действенных платформ анализа информации об угрозах безопасности.

Платформа анализа информации об угрозах автоматизирует, дополняет контекстом базовые сведения об угрозах – фиды (feeds). Фиды – это потоки данных с индикаторами компрометации, по которым распознается потенциальная угроза: хэши вредоносных файлов, IP-адреса и домены, связанные с преступной активностью. Автоматизация процесса освобождает перегруженный персонал, предоставляет точные средства для анализа в режиме реального времени, чтобы быстро и безошибочно реагировать на угрозы.

Платформы сбора оперативной информации об угрозах появились из-за количества доступных данных – как внутренних, так и полученных из внешних источников – о текущих и новых угрозах ИТ-безопасности. Компании, которые занимаются отслеживанием угроз, например, для обновления антивирусных продуктов, уже много лет ведут базы данных глобальных угроз, состоящие из программных агентов, работающих на миллионах клиентских компьютеров и других устройств. Эти данные вместе с фидами из других источников составляют инструменты платформ.

Что такое платформа анализа информации об угрозах

Платформа анализа угроз (*Threat Intelligence Platform*, *TIP*) – программное решение, используемое организациями для обнаруже-

ния, блокирования и устранения угроз информационной безопасности. Платформа объединяет несколько каналов сбора данных об угрозах, сравнивает с предыдущими событиями и генерирует оповещения для группы безопасности. TIP интегрируются с существующими решениями по управлению информацией и событиями безопасности (SIEM) и присваивают значения оповещениям, расставляя среди них приоритеты в соответствии с уровнем срочности.

К преимуществу платформы относится возможность команд информационной безопасности без опаски делиться информацией о кибербезопасности предприятия с другими отделами и внешними экспертами по безопасности. Система собирает и анализирует данные об угрозах, координируя тактику и действия заинтересованных сторон. Когда группа безопасности обнаруживает угрозу, к расследованию привлекаются все соответствующие департаменты. Благодаря этой способности синхронизировать действия и управлять усилиями, платформа незаменима в критические моменты.

Функции платформы

В отличие от фильмов, где действия хакеров приносят мгновенный вред, в жизни злоумышленники могут скрываться в вашей сети в течение долгого времени. В связи с этим безопасность меняет свой фокус с защиты и ответных действий на превентивные действия — не ликвидировать последствия атаки, а находить и устранять угрозы до нанесения какого-либо ущерба. Рассмотрим задачи, которые выполняет платформа.

• **Автоматизация рутинных задач и высвобождение времени.** Информация об угрозах должна входить в базовую часть надежных систем безопасности. По традиционной схеме информационной безопасности команды ведут итеративный поиск по сигналам тревоги, чтобы отличить реальные угрозы от ложных срабатываний, в то время как платформа поставляет группам уже обогащенную информацию для определения типа и степени серьезности угрозы, автоматически отбросив ложные оповещения.

• **Повышение точности вашей информации об угрозах.** Одна из причин, по которой люди плохо справляются с повторяющимися рутинными заданиями, «заключается» в том, что в какой-то момент глаза «замыливаются» и в конце концов случается ошибка обработки. Платформа сводит к нулю вероятность таких ошибок.

• **Нахождение собственных уязвимостей.** Часто команды безопасности больше беспокоятся о внешних угрозах, забывая о внутрен-

них. TIP ведет сканирование уязвимостей и предупреждает о слабых местах в вашей ИТ-инфраструктуре и сторонней экосистеме, помогая устранять слабые места на упреждение и укреплять систему.

• **Ускорение обработки данных.** Ручные процессы работы с данными трудоемкие и занимают много времени. Это становится решающим фактором во время атаки, когда нужна моментальная реакция, чтобы сдержать прорыв.

• **Обеспечение последовательного ответа на угрозы.** Автоматизированная платформа предоставляет соответствующую информацию по безопасности всем вовлеченным в процесс киберзащиты в компании. Это означает, что вся команда получает необходимую информацию одновременно, стратегия и процессы безопасности будут скоординированы.

Принцип работы

Платформы информации об угрозах выполняют три основные функции:

– агрегирование – сбор каналов, по которым информация об угрозах поступает в централизованный feed;

– анализ – обработка данных с использованием индикаторов определения и идентификации угроз безопасности;

– действие – уведомление о данных об угрозах групп реагирования на инциденты.

Эти функции реализуются платформой через автоматизацию рабочего процесса всего жизненного цикла системы безопасности. Рассмотрим этапы, связанные с жизненным циклом безопасности разведки угроз:

Сбор – суммирование данных из нескольких каналов, включая STIX, XML, JSON, OpenIOC. Важно включать данные из внутренних источников, таких как сетевые журналы, и из внешних источников, таких как Интернет и дарк-веб. Чем глубже и лучше фиды, тем действеннее платформа.

Корреляция – автоматизированный процесс TIP сортирует и организует данные с помощью метаданных тегов и удаляет несущественную или избыточную информацию. Затем идет сравнение с курируемой информацией, находятся закономерности и соответствия для обнаружения угроз.

Контекстуализация (контекст) – ключевой параметр в разведке угроз. Без него аномалию легко спутать с угрозой, и наоборот – не обратить внимания на реальную угрозу. На этом этапе TIP поставляет

контекст отсортированным данным для устранения ложных срабатываний, добавляя спецификации – IP-адреса, сеть и блок-списки доменов, обеспечивая команды как можно большим количеством информации о потенциальной угрозе.

Анализ угрозы – TIP анализирует индикаторы угроз в режиме реального времени на наличие взаимосвязи между данными. Далее эту информация можно «брать в оборот» аналитиками безопасности, чтобы находить скрытые угрозы.

Интеграция – платформы анализа угроз интегрируются с инструментами безопасности, используемыми организацией, для максимизации потока информации. На этом этапе платформа передает собранные и проанализированные данные в соответствующие отделы для обработки.

При обнаружении платформой угрозы посылается предупреждение группе информационной безопасности о необходимости запуска реагирования на инцидент.

Действие – эффективная платформа сбора оперативной информации об угрозах способна на ответные действия. Комплексные TIP сотрудничают с центрами обмена и анализа информации (ISAC) и организациями по обмену и анализу информации (ISAO), предоставляя им информацию, необходимую для разработки инструментов и приложений безопасности.

4.8. Методы и средства защиты информации

Средства защиты информации (СЗИ) – это собирательное название технических приборов, электрических или электронных систем и устройств, программных комплексов, а также прочих приспособлений для защиты информации.

Программно-аппаратная защита с использованием современных технических средств призвана снизить риск утечек, ограничив внутренний доступ к информационным системам.

Программно-аппаратные средства защиты – это способы контроля оборудования и программных средств от взлома, перехвата информации, несанкционированного подключения третьих лиц. Программные и технические средства защиты информации необходимы там, где утечка данных и ценной информации влечет за собой серьезные финансовые, репутационные, производственные риски для компании.

Средства защиты можно разбить на следующие группы:

– идентификация и аутентификация. Управление доступом;

– протоколирование и аудит;

– криптография;

– экранирование.

Идентификация и аутентификация. Управление доступом

Аутентификация – это основа безопасности любой системы, которая заключается в проверке подлинности данных о пользователе сервером.

Аутентификация не представляет собой ни идентификацию, ни авторизацию. Это три понятия, которые являются элементами защиты информации. Во-первых, идентификация, в процессе которой происходит распознавание информации о пользователе, его логине и пароле. Во-вторых, процесс проверки информации о пользователе – аутентификация. И, в-третьих, авторизация – проверка прав пользователя и определение возможности доступа.

Данная система защиты нужна для доступа к электронной почте, платежным системам, интернет-банкингу, форумам и социальным сетям.

Управление доступом – ограниченный доступ к информации, компьютерам, сетям, приложениям, системным ресурсам, файлам и программам. В основе управления доступом лежит идентификация и аутентификация. Задача управления доступом состоит в том, чтобы для каждой пары «субъект – объект» определить множество допустимых операций и контролировать выполнение установленного порядка.

Протоколирование и аудит

Протоколирование – сбор и накопление информации о событиях, происходящих в информационной сфере.

Аудит – это анализ накопленной информации, проводимый в реальном времени или периодически.

Данная система защиты выполняет важные задачи:

– составляет отчет обо всех пользователях и администраторах;

– выявляет слабые места в защите сервера, оценивает размер повреждений и возвращает к нормальной работе;

– предоставляет информацию для анализа и выявления проблем.

Характерной особенностью протоколирования и аудита является зависимость от других средств защиты информации. Идентификация и аутентификация служат началом для составления отчета о пользователях, управление доступом защищает конфиденциальность и целостность зарегистрированной информации.

Криптография

Криптографическая защита информации – это механизм защиты с помощью шифрования данных, в результате которого их содержание становится недоступным без предъявления ключа криптограммы и обратного преобразования.

Ключ – это важнейший компонент шифра, отвечающий за выбор преобразования, применяемого для зашифрования конкретного сообщения.

Криптографическими средствами защиты являются такие средства и способы преобразования информации, в результате которых скрывается ее содержание. Криптографическую защиту можно разделить на два основных вида: шифрование и кодирование защищаемых данных.

В случае шифрования каждый символ скрываемых данных подвергается самостоятельному преобразованию. Когда при кодировании защищаемых данных информация делится на блоки, имеющие смысловые значения, в результате каждый блок заменяется цифровым, буквенным или комбинированным кодом.

В состав криптографической системы входят: один или нескольких алгоритмов шифрования; ключи, используемые этими алгоритмами шифрования; подсистемы управления ключами; незашифрованный и зашифрованный тексты.

Экранирование

Экран – это средство разграничения доступа клиентов из одного множества информационных систем к серверам из другого множества посредством контроля информационных потоков между двумя множествами систем. Контроль потоков состоит в их фильтрации и выполнении некоторых преобразований.

Экран можно представить как последовательность фильтров. Каждый из фильтров, проанализировав данные, может пропустить или не пропустить их, преобразовать, передать часть данных на следующий фильтр или обработать данные от имени адресата и возвратить результат отправителю.

Главной функцией экранирования является обеспечение безопасности внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи.

Помимо функций разграничения доступа, экраны осуществляют протоколирование обмена информацией. Экранирование помогает поддерживать доступность сервисов защищаемой сети, уменьшая уязвимость внутренних сервисов безопасности.

Таким образом, наибольший эффект достигается тогда, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм защиты информации.

Механизм защиты должен проектироваться параллельно с созданием систем обработки данных, начиная с момента выработки общего замысла построения системы.

Функционирование механизма защиты должно планироваться и обеспечиваться наряду с планированием и обеспечением основных процессов автоматизированной обработки информации.

4.9. Экосистемный подход к кибербезопасности предприятия

Экосистемный подход к кибербезопасности предприятия – это интегрированное, комплексное использование различных инструментов, технологий и сервисов для защиты от цифровых угроз, где каждый элемент системы взаимосвязан и работает сообща для достижения общей цели безопасности. Такой подход позволяет повысить устойчивость, эффективность защиты и упростить управление всеми компонентами безопасности за счет синергии и стандартизации от одного или нескольких взаимосвязанных поставщиков.

Главным отличием промышленного предприятия является необходимость обеспечивать безопасность автоматизированных систем управления технологическим процессом, уязвимость которых может повлечь за собой нарушение технологического процесса.

Главные ключи к успеху в информационной безопасности для Индустрии 4.0 – превентивная оценка рисков и приоритет на безопасности в работе руководителей всех ключевых подразделений предприятия. Эти два аспекта следует «включать» от самых ранних стадий инсталляции любых технологических решений до окончания срока службы или вывода из эксплуатации.

Применение *экосистемного подхода* в построении единой цифровой экосистемы безопасности исключает ограничения, связанные с использованием технологий различных вендоров, и позволяет подойти к вопросам кибербезопасности комплексно, высвобождая тем самым ресурсы организаций на решение более приоритетных бизнес-процессов.

Отметим следующие преимущества экосистемного подхода перед использованием набора отдельных продуктов.

Все технологии экосистемы глубоко интегрированы и взаимосвязаны между собой, что позволяет решить задачи на стыке технологий, которые обычно остаются за пределами зон ответственности вендоров, и, как следствие, ложатся на инженеров Заказчика.

За счет *интеграции* и *тесной взаимосвязи* внутри экосистемы технологии обогащают друг друга дополнительными функциональными возможностями по аналитике, детектированию, реагированию, расследованию, проведению организационных мероприятий и комплексному управлению информационной безопасности. Этого очень сложно добиться при интеграции продуктов нескольких вендоров.

Экосистемный подход отличается своей гибкостью. То есть компании могут закупить и использовать лишь те технологии и в том объеме, который необходим на данном этапе и соответствует текущему уровню зрелости организации. Кроме того, экосистемы позволяют легко и безболезненно масштабироваться в будущем: поэтапно наращивать и расширять функционал SOC, дополняя его новыми технологиями по мере роста бизнеса и его потребностей. При внедрении экосистемы компании также получают долгосрочный план развития SOC и построения эффективной ИБ-защиты.

Благодаря комплексной поддержке работоспособности и связности технологий, все вопросы, связанные с эксплуатацией и развитием технологий экосистемы, решаются на стороне одного вендора. Сводятся к минимуму ситуации, при которых, например, после обновления версии одного продукта Заказчик неожиданно остается без подключенного к нему средства реагирования.

Таким образом, полезность экосистемного подхода к кибербезопасности заключается в наборе технологий и сервисов одной компании, дополняющих друг друга. И основное отличие экосистемы от набора продуктов заключается в том, что в экосистеме присутствует интеграционный слой, который позволяет открыто и прозрачно использовать все технологии без необходимости создания функциональных колодцев в виде воспроизведения работы одного компонента другим, как это было в примере с EDR.

SPF, DKIM и **DMARC** – эти технологии помогают защитить корпоративную почту от подделки и фишинговых атак.

SPF (Sender Policy Framework) позволяет владельцам доменов указывать, какие почтовые серверы имеют право отправлять почту от их имени. Это помогает предотвратить подделку адресов отправителей.

DKIM (DomainKeys Identified Mail) позволяет подписывать электронные письма криптографической подписью, что подтверждает их подлинность и целостность.

DMARC (Domain-based Message Authentication, Reporting & Conformance) строится на базе SPF и DKIM и позволяет владельцам доменов определять, как почтовые серверы должны обрабатывать сообщения, которые не прошли проверку подлинности. DMARC также предоставляет механизмы отчетности, позволяя организациям отслеживать попытки фишинга.

Двухфакторная аутентификация (2FA)

Внедрение 2FA существенно повышает безопасность. Даже если злоумышленник получит логин и пароль через фишинг, ему потребуется дополнительный код из SMS или приложения для доступа.

Для новых пользователей услуг Selectel 2FA включается автоматически. Проверьте, включена ли двухфакторная аутентификация у вас. Если нет, исправить это можно за несколько минут, следуя простой инструкции. В компании также предусмотрены различные способы получения кода для аутентификации. Это делает систему гибкой и удобной для пользователей.

Антифишинговые фильтры

Современные решения для фильтрации электронной почты помогают обнаруживать и блокировать фишинговые письма до того, как они попадут в почтовые ящики сотрудников. Фильтры могут распознавать фишинговые сообщения по URI-кодам и ключевым словам, а также использовать машинное обучение для выявления подозрительных писем.

Мониторинг DNS

Защита на уровне DNS блокирует доступ к опасным сайтам еще до того, как пользователь на них зайдет. Такие системы, как OpenDNS или Cloudflare, могут фильтровать DNS-запросы и автоматически блокировать подозрительные сайты.

Обучение сотрудников

Согласно исследованию, регулярное обучение может снизить вероятность успешного фишинга на 70 %. Некоторые компании проводят регулярные тренинги и учения, направленные на повышение осведомленности о киберугрозах. Например, в рамках учений сотрудники получают фальшивые фишинг-сообщения, которые им необходимо распознать. Эти тесты помогают выявить уровень готовности к реальным угрозам и обучить их правильным действиям в случае подозрительных писем.

Антивирус и системы мониторинга

Внедрение систем мониторинга сетевой активности позволяет выявлять аномалии и подозрительную активность в сети. Сюда входят попытки перенаправления трафика на фишинговые сайты. Антивирусные программы могут сканировать письма и вложения на наличие вредоносных файлов. Они блокируют их или предупреждают пользователя при обнаружении угрозы. Системы предотвращения утечек данных (DLP) помогают обнаруживать и блокировать передачу конфиденциальной информации вне организации. Это способствует предотвращению фишинговых атак.

Таким образом, к основным элементам экосистемы кибербезопасности относятся:

– системы обнаружения и предотвращения вторжений (IDS/IPS);
– решения для управления доступом и идентификацией (IAM);
– антивирусное ПО и решения для защиты конечных точек;
– средства защиты от целевого фишинга (spear phishing);
– механизмы изоляции браузера и безопасности контейнеров.

4.10. Тренды кибербезопасности 2025 года: анализ угроз и необходимые навыки специалистов

Ландшафт кибербезопасности сегодня складывается из нескольких взаимосвязанных направлений. С одной стороны, мы видим новые мотивы атакующих и новые техники, с другой – трансформацию самой цифровой среды, которая диктует появление новых точек входа. (Блог компании Positive Technologies/ А.Егоров.)

Политизация атак как новая реальность. Если раньше злоумышленники преследовали в первую очередь финансовую выгоду и выбирали отдельные компании в качестве целей, то с 2022 г. акценты сместились на государства и инфраструктуру целиком. В первой половине 2025 г. государственные учреждения оказались жертвами 21 % всех успешных атак на организации, и это максимальный показатель за последние годы. Основная цель таких кампаний состоит в дестабилизации: 68 % атак на госструктуры имели задачу нарушить их работу, а 29 % были направлены на причинение ущерба государственным интересам.

Атаки на цепочку поставок превратились в мультипликатор угроз. Чем быстрее развивается цифровизация, чем больше сервисов и приложений создается, тем выше становится риск закладки

вредоносного кода на этапе разработки. Злоумышленники используют это окно возможностей, они переходят от массового фишинга к целевым атакам на разработчиков. Их новая цель – цепочки поставок различных технологий. Внедряя вредоносное ПО в процессы разработки, злоумышленники наносят двойной удар: поражают не только саму жертву, но и проекты, с которыми она связана. Согласно исследованию, вредоносное программное обеспечение (ВПО) остается основным методом успешных атак на организации (используется в 63 % случаев). При этом доля распространения ВПО через сайты достигла 13 %. С помощью компрометации открытых репозиториев и тайпсквоттинга киберпреступники внедряются в цепочки поставок ПО. (*Тайпсквоттинг* – регистрация доменных имен, близких по написанию с адресами популярных сайтов в расчете на ошибку части пользователей.)

За счет этого растет интерес к DevSecOps и AppSec: компании вынуждены внедрять практики безопасной разработки, проверять код и тестировать продукты на уязвимости еще до релиза.

Облачная инфраструктура стала основной мишенью. Бизнесу дорого содержать собственное «железо», прогнозировать рост и закупать ресурсы впрок, поэтому сервисы массово переезжают в облака. Вместе с этим туда же перемещаются и атаки. Сегодня под ударом оказываются микросервисные приложения и облачные сервисы, которые стали частью критически значимой инфраструктуры компаний.

Искусственный интеллект изменил правила игры. Злоумышленники закладывают ИИ прямо во вредоносное ПО, и это позволяет вирусам действовать адаптивно. Попадая в новую среду, ВПО учится, перестраивает свое поведение и подбирает способы обхода защиты самостоятельно. Это упрощает разработку вредоносов и одновременно усложняет работу специалистов по информационной безопасности, поскольку стандартные методы детектирования перестают работать эффективно. Аналитика фиксирует резкий рост интереса ВПО: во II квартале 2025 г. доля атак с его использованием выросла до 76 %, на 26 процентных пунктов больше, чем кварталом ранее. Примеры вроде GIFTEDCROOK, который эволюционировал из простого стилера в инструмент кибершпионажа, показывают, насколько быстро ИИ меняет характер угроз.

Стиллер – это вирусное ПО, которое используется с целью того, чтобы украсть логины и пароли потенциальной жертвы. Когда инфицированная программа начинает работу, то сначала управление получает вирус. Вирус заражает другие программы, а также выполняет запланированные деструктивные действия.

Автоматизация SOC стала ответом на дефицит кадров. Масштабы цифровизации увеличивают число атак в геометрической прогрессии, а людей для реагирования катастрофически недостает. Поэтому в работу внедряют инструменты автоматизированного расследования, которые помогают фильтровать инциденты, выделять приоритетные и готовить аналитику для экспертов. Искусственный интеллект становится частью этой экосистемы, позволяя ускорить реагирование: человек принимает только финальное решение.

Социальная инженерия – основное оружие атакующих. Количество мошеннических схем с применением методов социальной инженерии растет экспоненциально. В первой половине 2025 г. на организации приходилось 50 % атак с использованием социальной инженерии, а на частных лиц целых 93 %. Основным каналом остается электронная почта, вместе с этим активно растет роль сайтов и мессенджеров. Мы видим, что человек стал ключевым звеном инфраструктуры, и именно он чаще всего становится слабым местом. Поэтому важно обучаться и повышать грамотность и кибергигиену.

Криптоактивы и Web3 создают новые векторы атак. Блокчейн развивается стремительно, капитал туда идет все активнее, и это делает его привлекательной целью. Web3 security становится самостоятельным направлением, требующим специфических инструментов и подходов.

Блокчейн – это децентрализованная система хранения и передачи данных, в которой они шифруются и объединяются в независимые блоки.

Эти тенденции вместе создают среду, где атаки становятся сложнее, быстрее и масштабнее одновременно. Мы видим рост числа атак на криптоактивы, появление новых вредоносов и расширение арсенала атакующих от вымогателей с функцией wiper, которые полностью стирают данные, до шпионских программ и кейлоггеров нового поколения. Именно в такой среде приходится строить защиту, и именно она определяет ключевые навыки, которые специалисту придется развивать.

Кейлоггер, или регистратор нажатий клавиш, – это программное или аппаратное средство, при помощи которого производится отслеживание и запись всех нажатий кнопок на клавиатуре компьютера или мобильного устройства. Они фиксируют вводимые пользователем данные, которые впоследствии могут передаваться злоумышленнику через Интернет или сохраняться на устройстве для последующего извлечения.

Какие навыки и инструменты нужны специалистам

Чтобы соответствовать этому уровню угроз, специалисту кроме знания базовой нормативной базы необходимо понимать, как компания зарабатывает деньги или осуществляет общественно важную функцию, и выстраивать защиту так, чтобы она сохраняла устойчивость и при этом оставалась эффективной с точки зрения процессов. Любое решение по усилению информационной безопасности обязательно должно учитывать бизнес-контекст.

Также специалисту по информационной безопасности важно всегда уметь мыслить, как атакующий. Хакер всегда делает первый ход, и карьера защитника напрямую зависит от того, насколько быстро он может адаптироваться к изменениям. Поэтому еще один ключевой навык состоит в способности учиться и перестраиваться вместе с изменением ландшафта угроз. Когда речь идет о сетях, DevOps-процессах или языках программирования, важно выходить за рамки поверхностного знания: нужно уметь строить защиту, которая реально работает, и глубоко понимать техническую сторону задач.

DevOps (от англ. *development & operations*) – методология автоматизации технологических процессов сборки, настройки и развертывания ПО. Она предполагает активное взаимодействие специалистов по разработке со специалистами по информационно-технологическому обслуживанию и взаимную интеграцию их технологических процессов друг в друга для обеспечения высокого качества программного продукта. Методология фокусируется на стандартизации окружений разработки с целью быстрого переноса ПО через стадии жизненного цикла ПО, способствуя быстрому выпуску версий программного продукта.

Современный специалист по информационной безопасности должен владеть инструментами анализа рисков и уметь просчитывать различные пути проникновения злоумышленника в инфраструктуру. На основании этого нужно прогнозировать действия атакующих и выстраивать защиту, направляя усилия именно туда, где они принесут максимальную пользу.

4.11. Риск-ориентированная модель информационной безопасности

Для получения результатов по кибербезопасности предприятия необходимо использовать *тренд риск-ориентированной модели информационной безопасности.*

Предлагаемая модель управления информационной безопасности на производстве строится на сервисном подходе и представляет собой экосистему следующих взаимоувязанных экспертных сервисов:

1) автоматизированное моделирование угроз безопасности;

2) анализ рисков информационной безопасности;

3) стендовое моделирование;

4) консалтинг.

Методологическая основа модели – сценарный подход к борьбе с киберугрозами: исходя из состава и устройства информационной инфраструктуры предприятия (или группы промышленных предприятий в составе холдинга), а также оценки критичности защищаемых сервисов и процессов формируется перечень возможных сценариев реализации угроз информационной безопасности, далее производится их ранжирование по степени потенциального ущерба, а потом стратегии, меры и средства нейтрализации выявленных угроз информационной безопасности формируются таким образом, чтобы исключить реализацию сценариев наиболее опасных угроз информационной безопасности (реализация которых наносит наибольший ущерб).

Риск-ориентированная модель обеспечения информационной безопасности промышленного сектора (https://cloudnetworks.ru/analitika/risk-orientirovannaya-model-obespecheniya-informatsionnoj/).

Рассмотрим компоненты модели подробнее.

1. Автоматизированное моделирование угроз информационной безопасности.

Моделирование угроз является основополагающим процессом при выстраивании защиты от угроз и выборе мер противодействия.

«Классическая» модель угроз, создаваемая по актуальной редакции Методики ФСТЭК России, оперирует следующими параметрами угроз информационной безопасности: источники и способы реализации; негативные последствия от реализации; возможные объекты воздействия; возможности реализации (возникновения). Это не в полной мере позволяет выявить совокупность факторов для полноценного прогнозирования возможных киберинцидентов.

Для последующего улучшенного прогнозирования возможных сценариев методологическая основа расширена и дополнена тактиками и техниками MITRE, позволяющими смоделировать сценарии реализации угроз, и базами уязвимостей CVE для более обширного охвата ландшафта угроз и способов их реализации.

В отличие от «классического» пути, объект автоматизации рассматривается в привязке к технологическим, производственным и

бизнес-процессам, а негативные последствия моделируются с учетом рассмотрения автоматизируемого технологического процесса.

Результатами моделирования являются перечень актуальных угроз и сценарии реализации киберинцидентов (kill-chain цепочки).

Фрагмент описания сценария реализации угрозы приведен в табл. 4.1. Полученные актуальные угрозы и сценарии реализации киберинцидентов являются основой для последующего анализа и формирования рисков информационной безопасности.

Таблица 4.1

Фрагмент описания сценария реализации угрозы

<table>
<tr><th colspan="4">Сценарий</th></tr>
<tr><td colspan="4">Нарушители: Преступные группы (криминальные структуры);
Группа сговора (Преступные группы (криминальные структуры);
Внутренние пользователи объекта защиты.
Вектор атаки: Получение НСД путем компрометации учетных данных
Результат: Несанкционированная модификация уставок технологического процесса с последующим аварийным остановом
Цепочка атаки: Корпоративный АРМ -> Сервер контроллера домена-> АРМ инженера (SCADA) -> ОРС-сервер -> ПЛК
Негативные последствия после наступления сценария:
Аварийное завершение технологического процесса с потерей промежуточного продукта.
Повреждение или утрата критически важных производственных данных.
Затраты на устранение последствий атаки и восстановление систем.
Риск аварийных ситуаций на производстве.
Нарушение работоспособности АСУ ТП.
Потеря визуального контроля за технологическим процессом, отсутствие возможности повлиять на его ход средствами автоматизации.</td></tr>
<tr><th>Паттерн нарушителя</th><th colspan="2">Точка входа</th><th>Целевой объект</th></tr>
<tr><td>Получение НСД путем компрометации учетных данных</td><td colspan="2">Корпоративный АРМ</td><td>Сервер контроллера домена;
АРМ инженера (SCADA)</td></tr>
<tr><th>Шаг 1</th><th colspan="3">Способы реализации</th></tr>
<tr><td>Получение НСД путем фишинга в корпоративный сегмент сети</td><td colspan="3">СП.2.3 Использование недостатков, связанных с отсутствием проверки достоверности отправителя и/или получателя
СП.13.4 Почтовый фишинг</td></tr>
</table>

2. Анализ рисков информационной безопасности.

Анализ рисков призван сформировать реестр рисков ИБ и дополнить, расширить и уточнить регуляторную составляющую в части выбора и приоритезации мер по обеспечению информационной безопасности.

Для создания реестра рисков информационной безопасности необходимо совместно с заказчиком сформировать шкалу оценки тяжести последствий, которая определяет границы приемлемости потенциального ущерба.

Далее, опираясь на выявленные сценарии реализации киберинцидентов и оценку величины потенциального ущерба, производят ранжирование рисков информационной безопасности на приемлемые и неприемлемые.

В рамках приоритезации направлений обеспечения информационной безопасности решаются следующие задачи:

– представление в денежном выражении последствий от инцидентов информационной безопасности;

– обоснование затрат на реализацию мер обеспечения информационной безопасности;

– присвоение приоритетов мероприятиям по защите информации;

– формирование (выбор) архитектур безопасности;

– целенаправленный выбор внедряемых средств защиты информации.

3. Стендовое моделирование.

С получением результатов анализа рисков совершается переход от методологической части вопроса к вопросу практической реализации мероприятий. Принимая во внимание требование высокой доступности сервисов автоматизации и особенностей АСУ ТП как объекта защиты от угроз информационной безопасности, немаловажной составляющей в успешной реализации мер является стендовое моделирование.

Использование стендов необходимо для практической апробации методик, проверки полученных в рамках риск-моделирования гипотез и выработки актуальных архитектур безопасности.

Стендовое моделирование призвано решить следующие задачи: своевременное выявление и анализ уязвимостей ПТК АСУ ТП в условиях обеспечения непрерывности производства;

– тестирование конфигураций безопасности и установление работоспособности ПТК АСУ ТП с настроенными механизмами безопасности;

– установление совместимости ПТК АСУ ТП и наложенных средств защиты информации.

В настоящее время сам процесс реализации технологической части стенда является очень «творческим», потому что действующими редакциями стандартов в области информационной безопасности и/или автоматизации никак не определены как понятие совместимости, так и параметры, позволяющие установить достаточность проработки стендовой модели, т. е. насколько подробно необходимо имитировать объект автоматизации.

В условиях неопределенности ключевых понятий и параметров мы полагаемся не только на собственный экспертный опыт, но и на опыт компаний-интеграторов АСУ ТП.

Таким образом:

– для установления совместимости наложенных средств защиты и ПТК АСУ ТП как таковой достаточно будет упрощенной технологической части стенда – приемлемо использование средств виртуализации (в том числе программируемые логические контроллеры) и автоматизации только фрагмента технологического процесса (одной ступени);

– для тестирования архитектур и политики безопасности необходимо создание подробной модели (с полной повторяемостью технологий информатизации и автоматизации) и имитации технологического процесса в области реализации технологической карты и алгоритмов.

Относительно недавно получило форсированное развитие направление цифровых двойников – «абсолютный» вариант с полной повторяемостью объекта автоматизации (структуры, свойств, информационных потоков). Исходя из главной особенности двойника, они более подходят для задач исследования защищенности.

Однако в рамках сценарного подхода оправдано использование *attack path analysis*, когда определяются потенциальные маршруты, по которым злоумышленники могут попытаться использовать уязвимости и проникнуть в рассматриваемую инфраструктуру. Указанный способ анализа путей атаки позволяет оценить потенциальное влияние рисков в результате реализации нескольких сценариев атаки, более эффективно выработать меры противодействия и обозначать приоритет их реализации.

4. Консалтинг.

Обозначенные выше факторы, тесная взаимосвязь бизнес-процессов, процессов производства и процесса обеспечения ИБ, единое пространство цифровой инфраструктуры предприятий дает все основания придать обеспечению информационной безопасности статус ключевого процесса. Для всех ключевых процессов очень важным фактором является стратегическое планирование.

Решения, принимаемые в рамках стратегического планирования, благодаря синергетическому эффекту, оказывают существенное (а порой и решающее) влияние на бизнес.

Соответственно, выбор правильной стратегии обеспечения информационной безопасности – залог устойчивости и бесперебойного функционирования критической инфраструктуры.

Предлагаемое в рамках риск-ориентированной модели методологическое обеспечение включает в себя услуги консалтинга.

Услуги консалтинга несут в себе следующие преимущества:

– долгосрочное планирование с учетом ключевых факторов, тенденций и прогнозов – системность и обоснованность принятия важных решений при обеспечении информационной безопасности;

– заказчик услуг получает в свое распоряжение лучшие практики по обеспечению информационной безопасности, апробированные ранее и доказавшие свою эффективность;

– достижение равновесного баланса сил и средств информационной безопасности – оптимальные траты на информационной безопасности при сохранении и поддержании должного уровня защищенности;

– обеспечение достигаемости результатов – только реальные цели и показатели, а также контроль исполняемости мероприятий на всех этапах реализации;

– независимость от конкретных поставщиков решений – мотивация консультанта не ориентирована на прибыль от продажи конкретного продукта и решения определенного производителя.

Формирование долгосрочной стратегии начинается с выявления состояния исходной защищенности и установления уровня зрелости компании.

Корректно определенные начальные параметры – залог достижения целевого состояния оптимальным путем. Последующие мероприятия, такие как аудит на соответствие требованиям и выявление уязвимостей, по сути являются поддерживающими.

Альтернативный подход – вероятностный – на данный момент нами не используется ввиду того, что для расчетов заявляемых метрик необходима обширная статистическая база по киберинцидентам в промышленном секторе. В настоящее время имеющаяся статистическая база не в полной мере обеспечивает методически корректное использование понятия вероятностей и не позволяет строить достоверную прогностическую модель, основанную на использовании понятия «вероятность реализации».

Возможно, в среднесрочной перспективе к реализации вероятностного подхода удастся вернуться благодаря реализации Industrial SOC и накоплению базы описаний киберинцидентов в промышленной инфраструктуре.

Заключение

В наши дни все крупнейшие нефтегазовые компании проводят активное сотрудничество с информационно-технологическими компаниями и создают собственные центры соответствующих цифровых компетенций. В зависимости от направления деятельности нефтегазовой компании и внедряемых цифровых технологий эффекты от цифровой трансформации будут разными, но в целом будет формироваться мульпликативный эффект для всей экономики, в частности, снижение затрат на разведку и добычу углеводородов, сокращение сроков ввода объектов в эксплуатацию, уменьшение численности персонала при удаленном исследовании объектов месторождения, автоматизации процессов управления оборудованием.

Данное учебное пособие способствует формированию у магистрантов-нефтяников умения понимать особенности процессов цифровой трансформации производственной деятельности. Представленный материал поможет расширить мировоззренческий кругозори освоить самостоятельно теоретические, практические и методические вопросы цифровизации, а также программные и технические средства информационных технологий, которые задействуются в процессах в нефтегазодобывающей промышленности.

В результате освоения дисциплин студенты *будут знать*: тенденции развития цифровых технологий в нефтегазовой отрасли; цифровые технологии, применяемые при разработке нефтегазовых месторождений; методологию принятия технических решений с использованием цифровых технологий. Наряду с этим студенты *смогут применять* современные цифровые технологии для решения профессиональных задач, а также *иметь навыки* применения цифровых технологий в нефтегазовой отрасли для повышения эффективности разработки.

Литература

1. Санкова, Л. В. Нефтегазовый комплекс на современном этапе: проблемы и перспективы цифровой трансформации / Л. В. Санкова // Актуальные проблемы экономики и менеджмента. – 2021. – № 1 (29). – С. 97–109.

2. Al-Fakih, A. Application of artificial intelligence in static formation temperature estimation / A. Al-Fakih, S. Kaka // Arabian Journal for Science and Engineering. – 2023. – Vol. 48. – P. 16791–16804. – DOI: 10.1007/s13369-023-08096-x

3. Application of machine learning in integrated modeling of the oil and gas fields / K. Pechko, A. Afanasyev, N. Brovin [et al.] // Third EAGE Digitalization Conference and Exhibition. – European Association of Geoscientists & Engineers, 2023. – P. 1–4. – DOI: 10.3997/2214-4609202332061

4. Оптимизация добычи: от продуктивного пласта до пункта подготовки нефти и газа // Э. Барбер, М. Е. Шиппен, С. Баруа [и др.] / Нефтегазовое обозрение. – 2008. – Т. 19, № 4. – С. 22–37.

5. End-to-end digital transformations for chemical companies. – URL: https://www.mckinsey.com (дата обращения: 01.05.2025).

6. Grieves, M. Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems / M. Grieves, J. Vickers // Systems Engineering. – 2017. – Vol. 20 (2). – P. 116–133.

7. IEC TR 63082-1:2020. Менеджмент интеллектуальных устройств. Ч. 1. Понятия и терминология (Intelligent device management – Part 1: Concepts and terminology.

8. ISO 8373:2012 Robots and robotic devices – Vocabulary. ISO/TC 299 Robotics, 2012 // International Organization. – URL: https://www.iso.org/-standard/55890.html.

9. Lee, J. A Cyber – Physical Systems Architecture for Industry 4.0 – Based Manufacturing Systems / J. Lee, B. Bagheri, H. A. Kao // Manufacturing Letters. – 2015. – Vol. 3. – P. 18–23.

10. Oil and Gas Leaders Taking Holistic Approach to Reinvention by Balancing Energy Security and Sustainability, Accenture Report Finds. – URL: https://newsroom.accenture.com (date of access: 01.05.2025).

11. Okon A. N. Explicit neural network-based models for bubble point pressure and oil formation volume factor prediction / A. N. Okon, A. J. Effiong, D. D. Daniel // Arabian Journal for Science and Engineering. – 2023. – Vol. 48. – P. 9221–9257. – DOI: 10.1007/s13369-022- 07240-3

12. Revolutionizing Oil & Gas: Digital Transformation Insights. – URL: https://www.birlasoft.com (date of access: 02.06.2025).

13. (2018). Data-driven smart manufacturing / F. Tao, Q. Qi, A. Liu, A. Kusiak // Journal of Manufacturing Systems. – 2018. – Vol. 48, P. 157–169.

14. Абишев, А. А. Перспективы цифровизации нефтяной отрасли Казахстана / А. А. Абишев, А. Е. Воробьев, Х. Тчаро // Вестник АУНГ (Казахстан). – 2018. – № 1 (45). – С. 37–46.

15. Азиева, Р. Х. Блокчейн-технология как ключевой элемент развития нефтегазовой индустрии / Р. Х. Азиева // Отходы и ресурсы. – 2020. – № 2. – URL: https://resources.today/PDF/06ECOR220.pdf (доступ свободный). Загл. с экрана. – DOI: 10.15862/06ECOR220

16. Азиева, Р. Х. Оценка экономического эффекта от использования цифровых технологий в нефтегазовой отрасли / Р. Х. Азиева // Креативная экономика. – 2022. – Т. 16, № 8. – С. 3225–3240.

17. Аминов, К. А. Цифровая трансформация нефтегазового комплекса как способ повышения эффективности производственных процессов в топливно-энергетическом секторе / К. А. Аминов, Ю. В. Лянду // Инновации и инвестиции. – 2023. – № 1. – С. 258–261.

18. Анисимова, Я. А. Перспективы цифровой трансформации в нефтяной промышленности / Я. А. Анисимова, В. А. Плотников // Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. – 2022. – Т. 12, № 5. – С. 106–119. – DOI: 10.21869/2223-1552-2022-12-5-106-119

19. Анализ перспектив развития цифровых технологий нефтегазовых месторождений / С. Г. Мухаметдинова, А. И. Коршунов, Н. О. Вахрушева, Т. Н. Иванова // Нефть. Газ. Новации. – 2022. – № 11. – С. 34–41.

20. Балахонова, И. В. Оценка цифровой зрелости как первый шаг цифровой трансформации процессов промышленного предприятия : монография / И. В. Балахонова. – Пенза : Изд-во ПГУ, 2021. – 276 с.

21. Байкова О. В. Эффекты цифровой трансформации в нефтегазовом комплексе / О. В. Байкова, Е. О. Громыко //Вестник университета. – 2021. – № 6. – С. 77–81.

22. Цифровая трансформация промышленности с помощью интернет-технологий / Е. А. Бахолдина, Н. С. Каретников, И. В. Ташник // Российский внешнеэкономический вестник. – 2018. – № 9. – С. 111–121.

23. Бекетова, О. Н. Стратегирование цифровой трансформации нефтегазовых предприятий / О. Н. Бекетова // Стратегирование: теория и практика. – 2023. – Т. 3, № 4. – С. 428–440. – DOI: 10.21603/2782-2435-2023-3-4-428-440

24. Соснок, А. «Белоруснефть»: по пути цифровизации / А. Соснок. – URL: https://www.neft.by/2023/09/26/belorusneft-po-puti-cifro-viza-cii/ (дата обращения: 12.04.2025).

25. Беспроводные технологии в «цифровом» нефтегазовом промысле. – URL: http://controleng.ru/besprovodny-e-tehnologii/tsifrovoe-mestoroz.

26. Бровка, Г. М. Информационная безопасность в таможенных органах : учеб.-метод. пособие для студентов специальности 1-96 01 01 «Таможенное дело» / Г. М. Бровка, И. А. Ковалькова, А. Н. Шавель. – Минск : БНТУ, 2019. – 118 с.

27. Бондаренко, Е. Обеспечение сетевой безопасности / Е. Бондаренко, М. Вихрева, П. Овчинникова. – URL: https://practicum.yandex.ru/blog/obespechenie-setevoj-bezopasnosti/2024.

28. Боровская, Е. В. Основы искусственного интеллекта : учеб. пособие / Е. В. Боровская, Н. А. Давыдова. – 4-е изд., электр. – М. : Лаб. знаний, 2020. – 130 с.

29. Будущее нефтегазовой отрасли через призму цифровых технологий / С. Ибрагимова, Д. Олимов, Ж. Салиев, Х. Ибрагимов. – URL: https://iais.uz/ru/outputnew/buduschee-neftegazovoy-otrasli-cherez-prizmu-tsifrovyh-tehnologiy (дата обращения: 29.01.2025).

30. Бутакова, И. Н. Функции SCADA, ERP, MES систем : лекция 2 по дисциплине «Системы оперативного управления производствами и предприятиями» / И. Н. Бутакова, П. А. Стрижак. – URL: https://portal.tpu.ru/SHARED/p/PAVELSPA/Study/Tab2/%D0%9B%D0%B5%D0%BA%D1%86%D0%B8%D1%8F_2.pdf.

31. Васнева, Е. Ф. Цифровые двойники в нефтегазовой отрасли [электр. изд.] / Е. Ф. Васнева // Цифровые технологии и информационная безопасность бизнес-процессов : сб. науч. ст. по итогам науч.-практ. конф., Н. Новгород, 25 мая 2022 г. / Нац. исслед. Нижегор. гос. ун-т им. Н. И. Лобачевского ; редкол. А. О. Грудзинский [и др.]. – Н. Новгород, 2022. – С. 15–19.

32. Велиев, Э. Ф. Интеллектуальное нефтегазовое месторождение на основе технологий искусственного интеллекта / Э. Ф. Велиев, Ш. В. Ширинов, Т. М. Маммедбейли // SOCAR Proceedings. – 2022. – № 4. – С. 70–75.

33. Величко, Л. Нефть в цифровом ландшафте / Л. Величко // Нефтяник Полесья. – 2024. – № 2 (46). – С. 40–53.

34. Власов, А. И. Потенциальные возможности создания интеллектуальных месторождений в Группе компаний «ЛУКОЙЛ»/ А. И.

Власов, К. В. Андреев, В. В. Поплыгин // Газовая промышленность. – 2014. – № 7. – С. 43–45.

35. Внедрение на промышленных предприятиях информационных технологий поддержки жизненного цикла продукции : метод. рекомендации / под ред. А. В. Тузикова. – Минск : Беларус. навука, 2012. – 189 с.

36. Воробьев, А. Е. Цифровизация нефтяной промышленности: базовые подходы и обоснование «интеллектуальных» технологий / А. Е. Воробьев, К. А. Воробьев // Вестник Евразийской науки. – 2018. – Т. 10, № 2. – URL: https://esj.today/PDF/88NZVN218.pdf (дата обращения: 05.05.2025).

37. Глухих, И. Н. Принятие решений на основе вывода по прецедентам в моделировании месторождений нефти и газа / И. Н. Глухих, Д. В. Никифоров // Вестник Тюменского государственного университета. Физико-математическое моделирование. Нефть, газ, энергетика. – 2019. – Т. 5, № 3. – С. 147–163. – DOI: 10.21684/2411-7978-2019-5-3-147-163

38. Горбов, И. А. Исследование драйверов цифровой трансформации нефтегазовой отрасли / И. А. Горбов, Е. С. Гаврилюк // Научный журнал НИУ ИТМО. Серия: Экономика и экологический менеджмент. – 2022. – № 2. – С. 49–62.

39. Горланов, С. Ф. Технический стандарт к системам погружной телеметрии УЭЦН-ключ к интеллектуализации процессов добычи нефти / С. Ф. Горланов, Ю. Ю. Шалагин // Оборудование и технологии для нефтегазового комплекса. – 2012. – № 3. – С. 86–91.

40. Система классификации и кодирования цифровой картографической информации : ГОСТ Р 51606-2000. – Введ. 01.01.2001. – М. : Гос. науч.-внедренч. центр геоинформ. систем и технологий, 2001.

41. Гульдемонд, Э. Организация и управления ИТ для «Умных месторождений» / Э. Гульдемонд, Л. Акда, М. Андронов // SPE 160557. – RU. – 2012.

42. Дайджест научно-технических публикаций по направлению: «Интеллектуальные месторождения». Второй квартал: 01.04.2022–10.06.2022. – М. : РГУ нефти и газа (НИУ) им. И. М. Губкина. – 54 с.

43. Епихин, А. О. Анализ жизненного цикла беспроводной сенсорной сети с использованием имитационного моделирования / А. О. Епихин, Р. В. Киричек, А. Е. Кучерявый // Актуальные проблемы инфотелекоммуникаций в науке и образовании : IV Междунар. науч.-техн. и науч.-метод. конф., Санкт-Петербург, 3–4 марта 2015 г. : в 2 т / Санкт-

Петербург гос. ун-т телекоммуникаций им. проф. Бонч-Бруевича. – СПб, 2015. – С.505–508.

44. Еремин, Н. А. Цифровой двойник в нефтегазовом производстве / Н. А. Еремин, А. Н. Еремин // Нефть. Газ. Новации. – 2018. – № 12 (217). – С. 14–17.

45. Об информации, информатизации и защите информации : Закон Респ. Беларусь от 10 нояб. 2008 г. № 455-З / Нац. правовой интернет-портал Респ. Беларусь. – Минск, 2008.

46. Информационно-аналитическая платформа для создания «Интеллектуального месторождения»: презентация. СибПроект Автоматика – URL: https://www.16oxy7p0h7.pdf – Яндекс Документы (дата обращения: 23.08.2025).

47. Казарин, О. В. Программно-аппаратные средства защиты информации / О. В. Казарин, А. С. Забабурин. – М. : Юрайт, 2017. – 312 с.

48. Карсаков, А. В., Процессы развития технологии нефтегазовой отрасли с использованием искусственного интеллекта / А. В. Карсаков, П. Н. Зятиков, И. В. Шарф // Известия Томского политехнического университета. Инжиниринг георесурсов. – 2025. – Т. 336, № 5. – С. 216–228. – DOI: 10.18799/24131830/2025/5/5048

49. Квинт, В. Л. Разработка стратегии: мониторинг и прогнозирование внутренней и внешней среды / В. Л. Квинт // Управленческое консультирование. – 2015. – Т. 79, № 7. – С. 6–11.

50. Кобзаренко, Д. Н. Анализ больших данных : учеб. пособие дисциплины для направления подготовки 38.03.05 «Бизнес информатика», профиль «Электронный бизнес» / Д. Н. Кобзаренко, А. Г. Мустафаев – Махачкала : ДГУНХ, 2019. – 107 с.

51. Концепция информационной безопасности Республики Беларусь (утв. Постановлением Совета безопасности Респ. Беларусь 18.03.2019 г. № 1).

52. Кореневская, А. В. Роботизация процессов в нефтегазовой отрасли Российской Федерации / А. В. Кореневская, Х. А. Пшиншев // Геополитика и экогеодинамика регионов. – 2020. – Т. 6 (16), вып. 4. – С. 281–289.

53. Куклина, Е. А. Стратегия цифровой трансформации как инструмент реализации бизнес-стратегии компании нефтегазового сектора современной России / Е. А. Куклина // Управленческое консультирование. – 2021. – № 6. – С. 40–53.

54. Куклина Е. А. Цифровые технологии как ключевой инструмент повышения эффективности нефтегазовой отрасли России в со-

временных условиях функционирования / Е. А. Куклина, Д. Н. Семкова // Управленческое консультирование. – 2020. – № 4. – С. 53–65.

55. Интеллектуальные системы в бурении скважин / А. Д. Кульбиков, Г. И. Кучукбаев, И. М. Нигматзянов // Инновации и инвестиции. – 2023. – № 7. – С. 172–175.

56. Удаленный мониторинг механизированного фонда скважин в ОАО «НК «Роснефть» / А. С. Малышев, А. А. Пашали, С. Е. Здольник, М. Г. Волков // Научно-технический вестник ОАО «НК «Роснефть». – 2009. – № 1. – С. 23–28.

57. Маргелов, Д. В. Месторождение на ладони – инновационный взгляд на перспективу интеллектуальных месторождений / Д. В. Маргелов // Инженерная практика. – 2010. – № 9. – С. 43–46.

58. МЭК 61987-11:2016. Измерения и управление в производственных процессах. Структуры и элементы данных в каталогах производственного оборудования. Ч. 11. Перечни свойств измерительного оборудования для электронного обмена данными.

59. МЭК 62769-1:2021. Интеграция полевых устройств (FDI). Ч. 1. Обзор.

60. Национальный стандарт РФ «Роботы и робототехнические устройства» : ГОСТ Р 60.0.0.4-2019/ИСО 8373:2012. Термины и определения, 2019. URL: http://docs.cntd.ru/document/1200162703 (дата обращения: 01.04.25).

61. Нормативно-правовые основы для реализации проектов по освоению информационных технологий в промышленности / Л. В. Губич, М. Я. Яковлев, Н. П. Муха, Г. П. Матюшенко // Информатика. – 2016. – № 2. – С. 88–103.

62. Об органе государственного управления в сфере цифрового развития и вопросах информатизации : Указ Президента Респ. Беларусь от 7 апр. 2022 г. № 136 – URL: https://president.gov.by/ru/documents/ukaz-no-136-ot-7-aprelya-2022-g (дата обращения: 01.06.25).

63. Об основных направлениях реализации цифровой повестки Евразийского экономического союза до 2025 года : решение Высш. Евраз. экон. совета № 12, 2017.

64. Основы ИИ: введение в искусственный интеллект. – URL: https://habr.com/ru/articles/865664/ (дата обращения: 18.04.2025).

65. Вывод на режим скважин, эксплуатируемых установками электроцентробежных и штанговых насосов с применением методов машинного обучения и цифровых двойников / А. А. Пашали, Д. В. Сильнов, А. С. Топольников [и др.] // Нефтяное хозяйство. – 2021. – № 7. – С. 112–117.

66. Цифровой двойник скважины как инструмент цифровизации вывода скважин на режим в ПАО АНК «Башнефть» / А. А. Пашали, А. В. Колонских, Р. С. Халфин [и др.] // Нефтяное хозяйство. – 2021. – № 3. – С. 80–85.

67. Пискунов, А. И. Вызовы, угрозы и ожидания цифровизации для промышленных предприятий / А. И. Пискунов // Организатор производства. – 2019. – Т. 27, № 2. – С. 7–15.

68. Информационные технологии. Интернет вещей промышленный. Общие положения предвар. нац. стандарт Рос. Федерации ПНСТ 642-2022 г. : утв. и введен в действие Приказом Росстандарта от 05.03.2022 г. № 18-пнст.

69. Прохорова, Т. В. Сервисы цифровых платформ для адаптивного управления / Т. В. Прохорова // Бизнес. Инновации. Экономика : сб. науч. ст. / Ин-т бизнеса БГУ. – Минск, 2023. – Вып. 7. – С. 145–151.

70. Интеллектуальные нефтегазопромысловые системы / И. Г. Соловьев, Д. А. Говорков, П. В. Кушманов, В. В. Фомин // Автоматизация, телемеханизация и связь в нефтяной промышленности. – 2016. – № 4. – С. 18–23.

71. Цифровая трансформация. Термины и определения : СТБ 2583–2020. – Минск : Гос. ком. по стандартизации, 2020. – 16 с.

72. Умный город. Термины и определения : СТБ 2622-2023. – Минск : Гос. ком. по стандартизации, 2023. – 16 с.

73. Интернет вещей. Термины и определения : СТБ 2623-2023. – Минск : Гос. ком. по стандартизации, 2023. – 18 с.

74. Сулейкин, А. С. Методы анализа и синтез архитектуры цифровых производственных экосистем / Сулейкин Александр Сергеевич : дис. ... канд. техн. наук. – М., 2022. – 128 с.

75. Сулоева, С. Б. Особенности цифровой трансформации предприятий нефтегазового комплекса / С. Б. Сулоева, В. С. Мартынатов // Организатор производства. – 2019. – № 2. – С. 28–36.

76. Филимонов, О. И. Экосистема как новая организационно-экономическая форма ведения виртуального бизнеса / О. И. Филимонов, Т. Г. Касьяненко, М. В. Кухта // Актуальные исследования. – 2021. – № 48 (75), ч. 2. – С. 31–41.

77. Ценжарик М. К. Цифровая трансформация компаний: стратегический анализ, факторы влияния и модели / М. К. Ценжарик, Ю. В. Крылова, В. И. Стешенко // Вестник Санкт-Петербургского университета. Экономика. – 2020. – Т. 36, № 3. – С. 390–420.– URL: https://doi.org/10.21638/spbu05.2020.303.

78. Белова, Я. С. Цифровая трансформация промышленных процессов / Я. С. Белова, А. М. Винокурова // Промышленность: экономика, управление, технологии. – 2022. – Т. 1, № 1 (1). – С. 8–14.

79. Цифровая трансформация. Основные понятия и терминология : сб. ст. / редкол.: А. В. Тузиков (пред.) [и др.] ; Нац. акад. наук Беларуси, Объед. ин-т проблем информатики. – Минск : Беларус. навука, 2020. – 267 с.

80. Эффективность цифровых технологий месторождений. – URL: https://belchemoil.by/news/analitika/cifrovaya-transformaciya-neftegazo-vogo-sektora (дата обращеня: 27.08.2025).

81. Яшин, Н. С. Методологические аспекты обеспечения устойчивости предприятия / Н. С. Яшин, Е. С. Григорян // Вестник Саратовского государственного социально-экономического университета. – 2014. – № 5 (54). – С. 113–117.

82. Якушев, Н. О. Вопросы исследования цифровизации в различных сферах деятельности / Н. О. Якушев // Цифровая трансформация. – 2024. – Т. 30, № 3. – С. 52–56. – URL: http://dx.doi.org/10.35596/1729-7648-2024-30-3-52-56.

83. Ховард, Р. Кибербезопасность: главные принципы / Р. Ховард. – СПб. : Питер, 2024. – 320 с.

84. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. – М. : Техносфера, 2023. – 782 с.

85. Цифровизация нефтегазового сектора в России и мире : кратк. обзор // Хабр [сайт]. − URL: https:// habr.com/ru/companies/online patent/articles/742636.

86. Практика применения ИИ в нефтегазовой отрасли / Russoft. − URL: https://russoft.org/-news/praktika-primeneniya-ii-v-neftegazovoj-otrasli.

87. Использование искусственного интеллекта и больших данных для оптимизации процессов в нефтегазовой отрасли / Дж. Мухаммедова, А. Гузычев, А. Аманова, М. Гылыджова // Инновационная наука. − 2023. − № 9-2. − URL: https://cyberleninka.ru/article/n/ispolzovanie-iskusstvennogo-intellekta-i-bolshih-dannyh-dlyaoptimizatsii-protsessov-v-neftegazovoy-otrasli.

88. Интернет вещей как платформа трансформации бизнес-моделей нефтегазовых компаний: инвестиционный анализ и оценка рисков / Общественно деловой научный журнал Энергетическая политики. − URL: https://energy-policy.ru/internet-veshhej-kak-platforma-transformaczii-biznes-modelejneftegazovyh-kompanij-investiczionnyj-analiz-i-oczenka-riskov/neft/2022/10/29.

89. Перспективы применения БПЛА в нефтегазовой отрасли: от геодезии до геологической разведки. − URL: https://integral- ~ 132 ~ russia.ru/2021/07/19/perspektivy-primeneniya-bpla-v-neftegazovoj-otrasli-ot-geodezii-dogeologicheskoj-razvedki.

90. Дроны в нефтегазовой отрасли: эффективный проект для автоматизации. − URL: https://ai-dron.ru/proekty-iidei/proekt_drona_dlja_neftegazovoj_otrasli.

91. VR и обучение персонала. За и против. − URL: https:// habr.com/ru/articles/730986.

92. Крылов, Д. Е. Виртуальная реальность в нефтегазовой отрасли / Д. Е. Крылов // Вестник науки и творчества. − 2024. − № 1 (92). − URL: https://cyberleninka.ru/article/n/virtualnaya-realnost-v-neftegazovoy-otrasli.

93. Промышленная кибербезопасность: итоги 2023 года. − URL: https://www.infowatch.ru/analytics/daydzhesty-i-obzory/promyshlennaya-kiberbezopasnostitogi-goda.

94. Вейс, Ю. В. Влияние VR технологий на эффективность производства в нефтегазовом комплексе / Ю. В. Вейс, Г. Д. Алфимов // Экономика и бизнес: теория и практика. – 2023. – № 5-1 (99). – С. 79–83.

95. Денисова, Т. С. Обзор VR/AR технологий и эффекты от их развития в РФ / Т. С. Денисова, А. А. Осипов // Молодежная школа-семинар по проблемам управления в технических системах имени А. А. Вавилова. – 2020. – Т. 1. – С. 8.

96. Жданова, Л. Е. Использование виртуальной реальности как инновационного метода обучения сотрудников предприятий нефтедобывающей отрасли / Л. Е. Жданова // Редакционная коллегия. – 2022. – С. 896.

97. Кузьмин, К. И. Роль виртуальной реальности в оптимизации производственных процессов и обеспечении безопасности персонала на примере нефтегазовой отрасли / К. И. Кузьмин // Прогрессивная экономика. – 2023. – № 6. – С. 5–14.

98. Крылов, Д. Е. Виртуальная реальность в нефтегазовой отрасли / Д. Е. Крылов // Вестник науки и творчества. – 2024. – № 1 (92). – С. 5–9.

99. Какие разработки двигают нефтегазовую отрасль вперед. − URL: https://www.vedomosti.ru/partner/articles/2023/02/08/961921-razrabotki-dvigayut.

100. Невзорова, А. Б. Системы управления нефтедобывающей компании для контроля производственных процессов / А. Б. Невзорова, Е. В. Коробейникова, В. В. Фролов // Нефтегазовый инжиниринг. – 2025. – № 2 (3). – С. 7–15.

Учебное электронное издание комбинированного распространения

Учебное издание

Невзорова Алла Брониславовна

ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ПРОИЗВОДСТВЕННЫХ ПРОЦЕССОВ НЕФТЕДОБЫВАЮЩЕЙ ОТРАСЛИ

Учебное пособие

Электронный аналог печатного издания

Редактор *Н. Г. Мансурова*
Компьютерная верстка *И. П. Минина*

Подписано в печать 30.12.25.
Формат 60x84/16. Бумага офсетная. Гарнитура «Таймс».
Ризография. Усл. печ. л. 11,16. Уч.-изд. л. 11,6.
Изд. № 760/74.
http://www.gstu.by

Издатель и полиграфическое исполнение
Гомельский государственный
технический университет имени П. О. Сухого.
Свидетельство о гос. регистрации в качестве издателя
печатных изданий за № 1/273 от 04.04.2014 г.
пр. Октября, 48, 246746, г. Гомель